

TAG Cyber  
**Security Annual**  
2ND QUARTER 2022



# CYBERWAR

A S P E C I A L I S S U E

ARTICLES / OPINIONS / INTERVIEWS

## WELCOME TO THE 2022 TAG CYBER SECURITY ANNUAL 2ND QUARTER EDITION

---



LESTER GOODMAN,  
DIRECTOR OF CONTENT,  
TAG CYBER

**A**s I type these words in early April 2022, Vladimir Putin continues to bombard the cities and citizens of Ukraine in what is certainly the most important conflict in Europe since World War II.

And as people around the world watch the daily news with growing horror, the previously esoteric issue of cyberwarfare has emerged as a kitchen-table discussion topic, arguably on par with the nuclear and biological threat in its potential consequence to humans.

In this 2022 TAG Cybersecurity Annual— 2nd Quarter Edition, we tackle the topic of cyberwar from several different perspectives. On the one hand, we try to help readers understand how a cyberwarfare conflict might actually play out. This is necessary to bring cyberwar out from the pages of textbooks and onto the doorsteps of every citizen.

On the other hand, we try to offer dispassionate views of how cyberwar must be addressed by businesses, governments, citizens and technology providers. We do this in the voice of our expert TAG Cyber analysts—perhaps the most experienced assembly of experience and talent in cybersecurity in the world.

Be warned: This volume is uncomfortable reading. From our illustrated depiction of a feasible warfare scenario to Dr. Amoroso’s chilling argument that patterns predict that a global cyberwar will emerge by 2036, this volume will have you shifting in your seat.

But I hope you will spend time with this work. Read the feature articles and check out the interviews with the cybersecurity technology leaders included in the volume. Note that we asked each one to comment on cyberwarfare; it’s enlightening to see what they believe.

As always, we hope that you will benefit from our research—and we thank our Research as a Service (RaaS) customers in enterprise and our Content as a Service (Caas) customers in the security vendor community for providing the support to enable our research and writing. It is through their kind support that we can offer this volume to readers for free.

Let’s all hope that by the time this volume hits the press in mid-April, tensions will have subsided and the Ukrainian people can return to their homes. Let’s hope that by the time you read these words, peace has returned to the region, and children can sleep safely with their families.

But regardless of what happens in Ukraine, the lessons learned from the conflict and their relationship to cybersecurity and cyberwarfare must not be ignored.

I hope you and your team will benefit from this volume, and let’s all hope for peace.

Lester Goodman, Director of Content

David Hechler, Editor

#### Contributors

Ed Amoroso  
Jennifer Bayuk  
David Hechler  
Jessica Andrus Lindstrom  
John Masserini  
Gary McAlum  
Christopher R. Wilder

#### Editorial & Creative

Lester Goodman  
David Hechler  
Judy Lopatin  
Miles McDonald  
Rich Powell

#### Research & Development

Matt Amoroso  
Shawn Hopkins

#### Sales & Customer Relations

Rick Friedel  
Trish Vatis  
Laurie Mushinsky

#### Marketing

Scott Krady  
Tony Taddei  
Leona Laurie

#### Administration

Liam Baglivo  
Julia Almazova

Ed Amoroso, Founder & CEO



Volume 8 No. 2

TAG Cyber LLC  
P.O. Box 260, Sparta, New Jersey 07871  
Copyright © 2022 TAG Cyber LLC. All rights reserved.

This publication may be freely reproduced, freely quoted, freely distributed, or freely transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system without need to request permission from the publisher, so long as the content is neither changed nor attributed to a different source.

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

Neither the authors of this document nor TAG Cyber LLC assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the 2022 TAG Cyber Security Annual volumes.

The opinions, information, advice, and recommendations expressed in this publication are not representations of fact, and are subject to change without notice. TAG Cyber LLC reserves the right to change its policies or explanations of its policies at any time without notice.

**The opinions expressed in this document are that of the TAG Cyber Analysts, and in no way reflect that of its Distinguished Vendors.**

April 15, 2022

C O N T E N T S

Introduction	2	Managing Security for SMBs Corey White, Cyvatar	63
<b>CYBERWAR</b>	<b>5</b>	Browser Isolation as a Key Enterprise Security Control Henry Harrison, Garrison Technology	66
Using Time Patterns to Predict Future Cybercampaigns Edward Amoroso	6	Scanning GitHub for Vulnerabilities and Secrets Ziad Ghalleb, GitGuardian	69
A Short History of ‘Cyberwar’ Jessica Andrus Lindstrom	10	Continuous Management of Cyber Assets and Controls Paul Ayers, Noetic Cyber	72
What the International Legal Experts Say about Cyberwar David Hechler	15	Preventing Abuse of APIs Cameron Galbraith, Noname Security	75
Death to Esporontia! – Part I Christopher R. Wilder & Lester Goodman	20	Extending Zero Trust Data Access to the Enterprise Larry Hurtado, Qnext	77
Death to Esporontia! – Part II Christopher R. Wilder	23	Securing Code During Devops Liran Tancman, Rezilion	80
CyberWar...the Day After Gary McAlum	29	Using Breach and Attack Simulation to Reduce Cyber Risk Itzik Kotler, SafeBreach	82
The Founder of a Cyberwar Journal Talks About Ukraine (and More) David Hechler	33	Reducing Cyber Risk for Modern Apis Roey Eliyahu, Salt Security	85
Cybersecurity Tool Portfolio—Friend or Foe? Jennifer Bayuk	36	Advancing Cyber Hygiene for Enterprise Rita Gurevich, Sphere Technology Solutions	87
A New Ecosystem of Alliances David Hechler	40	Application Detection and Response David Movshovitz, TrackerDetect	90
<b>INTERVIEWS</b>	<b>44</b>	<b>ANALYST REPORTS</b>	<b>93</b>
Unifying Cyber Protections Across the Enterprise Candid Wüest, Acronis	45	A Maturity Model for Access Controls to Improve Cyber Hygiene	94
An Early Warning Service for Cybersecurity Juha Haaga, Arctic Security	47	Evidencing Cyber Resilience via Simulations and Scenarios: An Overview of Immersive Labs	100
Ensuring Security Focus Across Devops Guy Flechter, Cider Security	50	Protecting the Everywhere Workplace: An Overview of Ivanti Cybersecurity	105
Safeguard Your People, Data, and Brand Through Digital Risk Protection Services Kailash Ambwani, Constella Intelligence	52	Risk-Based Management of Third-Party Cybersecurity Exposures: An Overview of Prevalent	110
Supporting Compliance as a Service Kishor Vaswani, ControlCase	55	Integrating Cybersecurity Support for Home and Small Business Into Telecom Service Infrastructure	118
Leveraging The Power of Open Source-Based Network Detection and Response Brian Dye, Corelight	57		
Managing Third-Party Cyber Risk Fred Kneip, CyberGRX	60	<b>DISTINGUISHED VENDORS</b>	<b>141</b>



A SPECIAL ISSUE

# CYBERWAR

# USING TIME PATTERNS TO PREDICT FUTURE CYBERCAMPAIGNS

EDWARD AMOROSO

By extrapolating the average time between initial cyber skirmishes and their corresponding full-out attack campaigns, disturbing predictions can be made about future industrial control system attacks, artificial intelligence misuse and global cyberwar.

## USING MODELS TO PREDICT ATTACK CAMPAIGNS

During the past quarter-century, a pattern has emerged in which some new cyberattack method is demonstrated to work in the wild and, after a period of relative calm, is then fully exploited at scale roughly 13 years after the initial view. This broad pattern has applied to worms, distributed denial of service (DDOS) and ransomware.

Using simple extrapolation, it becomes possible to make predictions about future attack campaigns at scale, based on initial observations currently experiencing relative calm. Specifically, disturbing predictions can be made about industrial control system (ICS) attacks, artificial intelligence (AI) misuse, and global cyberwar.

### MODEL 1: WORMS

The first worm<sup>1</sup> was observed in 1988 through the so-called Morris Worm. In the ensuing years, worms were certainly known, but it was not until 15 years later, in 2003 that the method was deployed at scale. During that year, the SQL/Slammer, Blaster, Nachi and Sasser worms were unleashed against global infrastructure.



Figure 1. Worm Pattern

## MODEL 2: DDOS

The first recognition of the DDOS threat came via warnings from the U.S. federal government in advance of the Y2K transition. Serious DDOS attacks followed in March 2000 targeting CNN, eBay and others. After a relatively quiet period of 12 years, a full unleashing of DDOS fury was aimed at U.S. online banks in 2012, presumably from a nation-state actor.

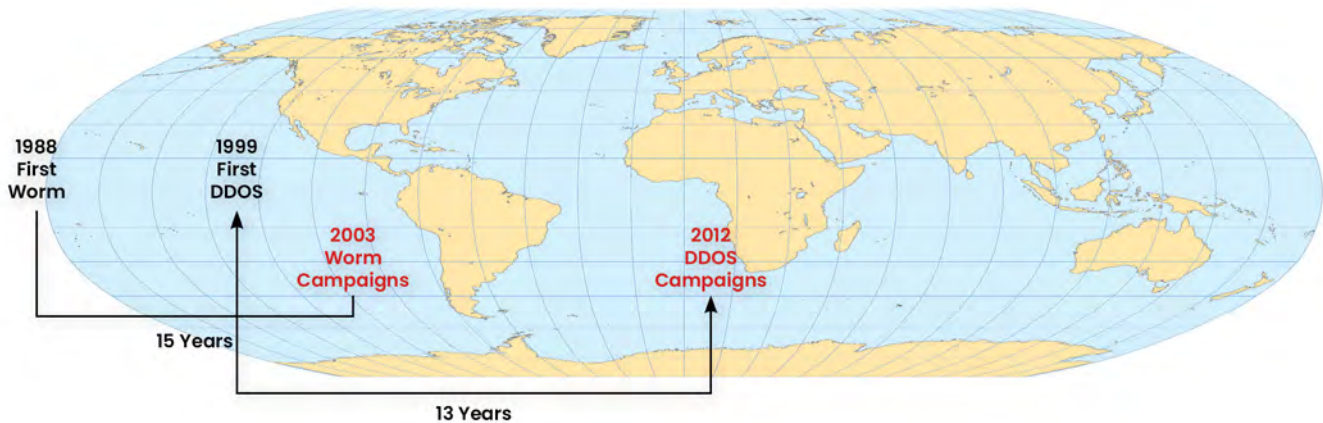


Figure 2. Adding DDOS Pattern

## MODEL 3: RANSOMWARE

The first evidence that cryptocurrency could be used for illicit purposes emerged in 2008 with the famous Bitcoin paper. After a period of unease with cryptocurrency, including isolated issues such as Silk Road, the first broad exploitation emerged with ransomware attacks, which reached a peak in 2020 (and continue today).

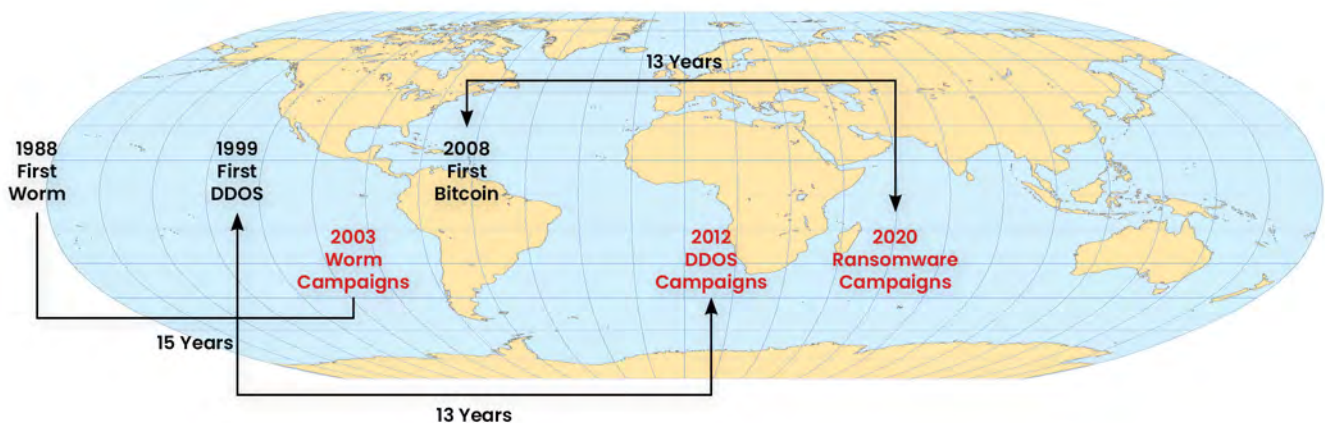


Figure 3. Adding Ransomware Pattern

## MODEL 4: ICS ATTACK

The first serious industrial control system (ICS) attack of any real consequence occurred in 2010 with the famous Stuxnet incident, which targeted Iranian nuclear systems. Extrapolating forward, one can predict that a series of disturbing ICS attacks is likely to occur in the coming year, possibly in 2023. Citizens should expect to see hits to factories, power systems, and so on.

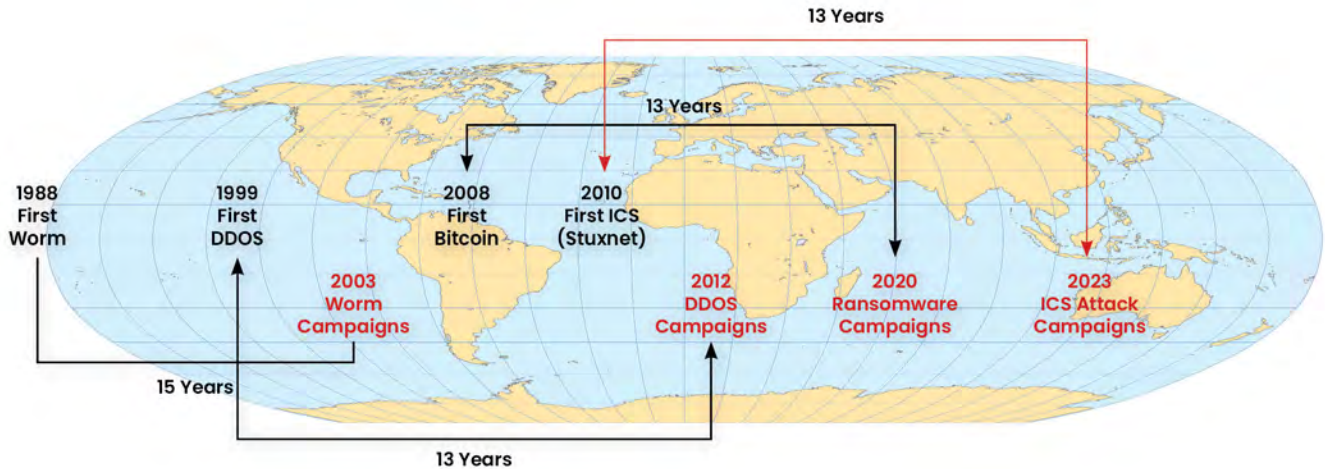


Figure 4. Adding ICS Attack Pattern

## MODEL 5: AI MISUSE

The first evidence that AI could be applied to cybersecurity emerged in roughly 2013 with the emergence of companies like Cylance. While this is a benign initial view, one can easily extrapolate misuse of AI to emerge at scale in roughly 2028, which is 15 years after the first occurrence. Citizens should expect to see AI offensive weapons that use AI models for attacks.

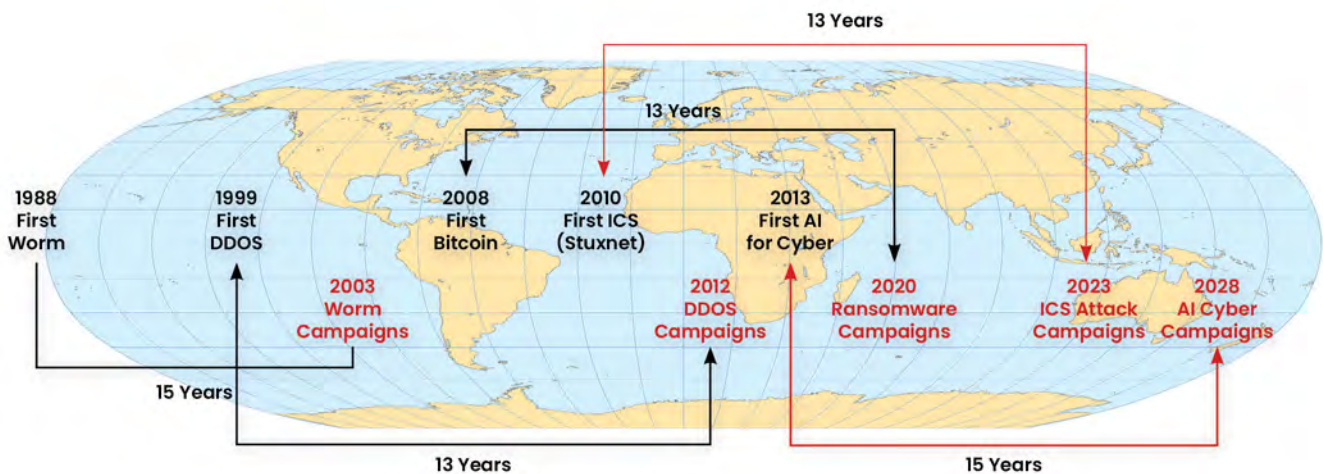


Figure 5. Adding AI Misuse Pattern



## MODEL 6: GLOBAL CYBERWAR

The current situation between Russia and Ukraine is more than likely to cascade into a serious cyberwarfare situation where the goal is serious cyber dominance, versus making a political or philosophical statement. Extrapolating this geopolitical conflict using our pattern model puts the first global cyberwar 14 years later, in 2036.

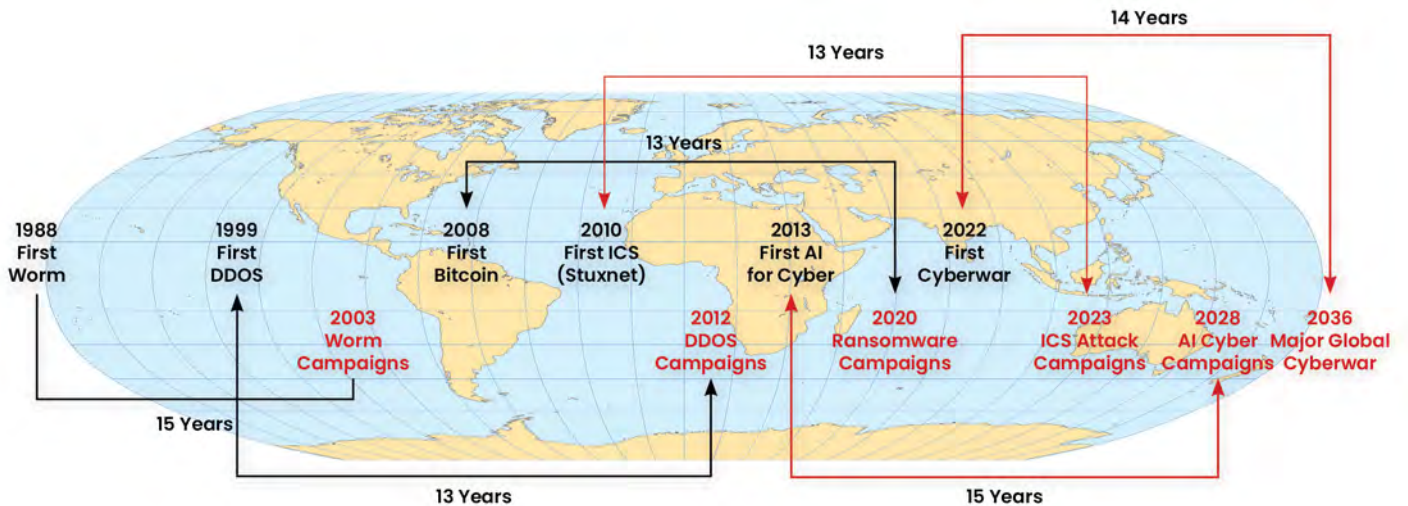


Figure 6. Adding Global Cyberwar Pattern

## IMPLICATIONS

Readers will note that no interpretation is made here beyond the simple pattern matching and extrapolation done based on previous and existing data. Nothing about the predictions of ICS attacks, AI misuse and global cyberwarfare should raise an eyebrow for any expert observer. All of these possibilities seem high, and we should view such campaign predictions as grave.

<sup>1</sup> Readers might quibble with the author's designation of what was actually the first observation of a given attack method. Every effort is made to select prominent, meaningful first observations that a given method can work in the wild. Usually, if some other exploitation would have been selected, its emergence date is sufficiently adjacent as to not change the average 13-year thesis proposed here.

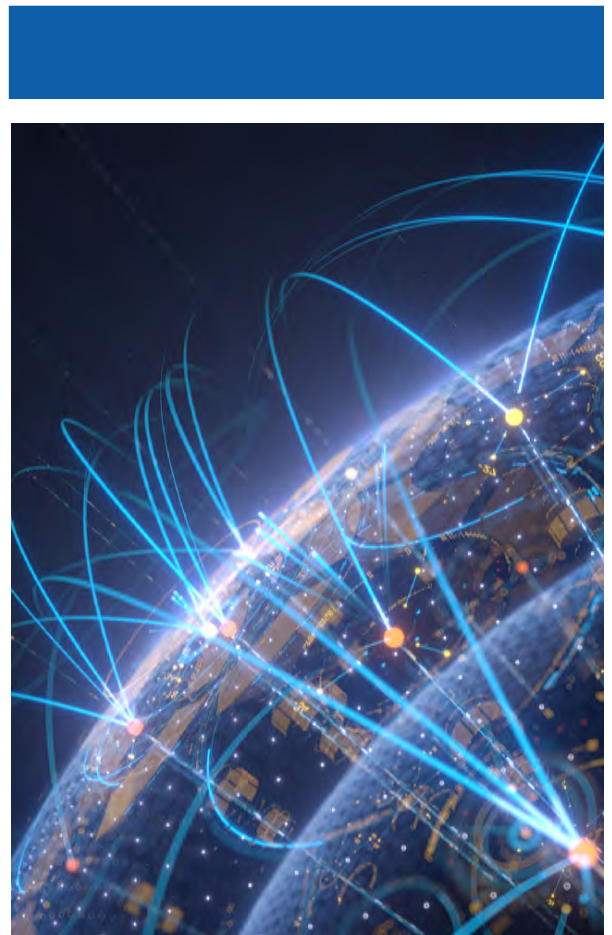
# A SHORT HISTORY OF ‘CYBERWAR’

JESSICA ANDRUS LINDSTROM

What is cyberwar? From the debate and discourse that have populated scholastic and journalistic writing for years, it's clear that not everyone in the cybersecurity field agrees on what a cyberwar is—or even if cyberattacks and operations should be defined as war at all. Back in 2010 in their book “Cyberwar: The Next Threat to National Security,” Richard Clarke (former counterterrorism adviser to presidents Bill Clinton and George W. Bush) and Robert Knake defined the concept of a war waged by cyber as “actions by a nation-state to penetrate another nation’s computers or networks for the purpose of causing damage or disruption.” Two years later in his book “Cyberwar Will Not Take Place,” Thomas Rid, a professor at Johns Hopkins University’s School of Advanced International Studies, cautioned scholars and military strategists against using the term “war” to describe what he viewed as nonviolent computer breaches that could be a prelude to more traditional, kinetic warfare but were used primarily for “sabotage, espionage, and subversion (undermining established authority).” Yet even with Rid’s admonishment, the term continued to proliferate within academic papers and military reports, and with its repeated use, the understanding of “war” and its usual associations with death and destruction evolved into something much more complex. Most experts in the field today, including Rid, seem to agree that computer breaches used to sabotage and subvert have become an integral part of warfare.

It’s hard to pin down exactly when the concept of cyberwar surfaced in the world of nonfiction. (As we will see, developing notions of cyberwar first appeared years earlier in fantasy and science fiction books, movies and TV shows, which were profoundly influential.) In January 1987, “Cyberwar” appeared in Omni magazine as the title of an essay by Owen Davies. Oddly, the term itself did not appear in the article. It described real world confrontations that included drones used for surveillance (Israel versus Syria in 1982–

**“Before spaceships existed, before AI became a reality, before cyber highways and simulated war gaming became known entities, they existed first as fantasy.”**



83) and artificial intelligence used in traditional combat (Falklands War, 1982). But the topic emerged as a serious subject of study only after the launch of another war a few years later.

## IT BEGAN WITH THE GULF WAR

In 1991, James Der Derian presented a paper in which he talked about the Gulf War at a cyberspace conference. Now the director of the Centre for International Security Studies at the University of Sydney, Der Derian included that paper, “Cyberwar, Videogames and the Gulf War,” as the last chapter of a book he published a year later. In the chapter, he used video game analogies to describe the Gulf War and argued that “the technical, preparation, execution and reproduction of the Gulf War created a new virtual—and consensual—reality: the first cyberwar, in the sense of a technologically generated, televisually linked, and strategically gamed form of violence that dominated the formulation as well as the representation of US policy in the Gulf.”

A year after the publication of Der Derian’s book (“Antidiplomacy: Spies, Terror, Speed, and War”), John Arquilla and David Ronfeldt published an article called “Cyberwar is Coming.” Arquilla was a professor of defense analysis at the Naval Postgraduate School and a consultant to General Norman Schwarzkopf during the Gulf War, and Ronfeldt was a senior social scientist at RAND. Their article became a chapter in a book they edited called “Athena’s Camp: Preparing for Conflict in the Information Age.” One sentence reverberated throughout the scholastic and military world: “Cyberwar may be to the 21st Century what blitzkrieg was to the 20th.”

The topic became a hot one, and multiple essays, articles and books about information war and cyberwar followed as journalists and academicians came to grips with new cyberattacks occurring with more frequency and severity. In 2000, during violent clashes between Palestinians and Israelis, Israeli government websites were attacked. Hackers penetrated the Bank of Israel and the Tel Aviv Stock Exchange, and more than 100 websites were disrupted. Not all of the perpetrators were local. Pro-Palestinian and pro-Israeli individuals from as far away as South America participated in the conflict. Analyzing these attacks in her 2001 article “Cyberwarriors: Activists and Terrorists Turn to Cyberspace,” Georgetown University’s computer science professor Dorothy Denning wrote: “The Israeli-Palestinian cyberwar illustrates a growing trend. Cyberspace is increasingly used as a digital battle-ground for rebels, freedom fighters, terrorists, and others who employ hacking tools to protest and participate in broader conflicts.”

A decade later came a highly sophisticated attack that underscored the new power of cyberweapons. The Stuxnet worm was unleashed to infiltrate and incapacitate Iran’s nuclear program. Purportedly the combined work of U.S. and Israeli intelligence, the Stuxnet malware temporarily halted Iran’s effort to build a nuclear weapon. Journalist Kim Vetter analyzed the implications in her 2015 book “Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon.” In describing the attack and its aftermath, Vetter concluded that a new age of warfare had emerged. The potential for devastation via cyber, she wrote, rivaled that of nuclear weapons.

Vetter’s vision was timely. When her book went to press in 2015, a more powerful attack was in the works. This one appeared to be a nation-state targeting another nation-state with the clear intent of debilitating the defenses of the targeted country by incapacitating its infrastructure. Over a period of three years, hackers (later identified as Russian military intelligence officers and indicted by the U.S. government in 2020) released crippling malware, beginning with Black Energy, to disrupt Ukraine’s power infrastructure. Other, more malicious, malware like the NotPetya worm and Olympic Destroyer followed and ended up affecting countless global computer systems, including those used by authorities at the 2018 Winter Olympics in South Korea.

The economic cost of these attacks was an estimated \$10 billion. And it could have been worse. Had

Ukraine not had the capability of turning its power grids back on manually, there could have been human casualties. “It is clear where the world is going,” Andy Greenberg wrote in his book “Sandworm.” “We’re entering a world where every thermostat, every electrical heater, every air conditioner, every power plant, every medical device, every hospital, every traffic light, every automobile will be connected to the Internet. Think about what it will mean for the world when those devices are the subject of attack.”

NotPetya captured the world’s attention. Cyberattacks were no longer isolated events in a small corner of the globe. Directly and indirectly they could affect millions of people in dozens of countries. It was time to start planning to defend against the next attacks.

Such attacks as hypotheticals abounded in Clarke and Knake’s book. Though it was written almost a decade before “Sandworm” appeared in 2019, “Cyberwar: The Next Threat to National Security” described worst-case scenario cyberwars that could destroy a country not with physical deployment of nuclear bombs, but with anonymous computer attacks that would guarantee the gradual, calculated crippling of a nation’s infrastructure by another nation or by terrorists, leaving the citizens under attack literally and figuratively dying in the dark.

## FANTASY CAME FIRST

Such hypotheticals probably seemed like fiction to many readers back in 2010, but there were those like James Der Derian who maintained that fiction was where many of the concepts and images associated with cyberwar began. Before spaceships existed, before AI became a reality, before cyber highways and simulated war gaming became known entities, they existed first as fantasy. From H.G. Wells describing time travel and attacks by Martians in the 1890s to Isaac Asimov creating robotic literature in the 1940s, sci-fi writers imagined the unimaginable. In the ‘50s, Kurt Vonnegut, Jr. and Robert Sheckley produced tales of computers built for waging war and silent guns that could vaporize humans with no bloodshed. Stories like these had the capacity to titillate as well as terrify. It was science fiction, Der Derian asserted in “Cyberwar, Video Games, and the Gulf War,” that first “alerted us to the dangers of cyberspace.”

Following the Martian-themed, robotic warfare of the late 19th and early 20th century, sci-fi themes of space travel, intergalactic battles and tyrannical colonization proliferated in the 1960s and ‘70s. One book turned out to have a fan base among current hackers: Frank Herbert’s “Dune,” the 1965 sci-fi epic of interstellar travel and colonization. The connection was uncovered during the investigation of an attack on Ukraine’s energy grid. In 2014, a private intelligence agency was working to establish attribution of the BlackEnergy malware that had infected a computer in Ukraine—malware that would later be associated with the NotPetya attack. Initially the analysts discovered instructions in the code written in Russian. Then they found tags in the malware that would allow the hackers to sort and track computers they’d infected. As they delved deeper, they realized that those tags were names from “Dune.” The more they delved, the more associations and references to the novel they uncovered. The hackers were clearly fans. When it came time for the investigators to give the hackers a name, they thought of one of the most memorable characters in the book—the hideous, oversized sandworms that lived beneath the surface of the planet’s vast desert. Sandworm is what the investigators called the gang now believed to be Russian military intelligence officers, and what Greenberg titled the book in which he traced their exploits.

Much more than just names and characters became associated with modern cyber concepts in the “Star Trek” series beginning in the 1960s. Uncannily, “Star Trek” appeared in many instances to predict accurately future scientific inventions and engineering breakthroughs like computer tablets, Bluetooth headphones and cellular phones, to name but three. Although the term “cyberwar” was never used, specific episodes hinted at cyber capabilities, from the use of GPS and simulated wars in “A Taste of Armageddon” (1967 season 1, episode 23) to the piloting of the USS Enterprise by a computer that takes over the ship during Star

Fleet war games in "The Ultimate Computer" (1968 season 2, episode 24). Another computer acted as the antagonist in taking over a spaceship in Stanley Kubrick's "2001: A Space Odyssey." He was, of course, HAL 9000. Also appearing that same year (1968) was a short story by the prolific sci-fi writer Philip K. Dick. That story, "Do Androids Dream of Electric Sheep?," was adapted for the screen in 1982 as the movie "Blade Runner," which teemed with bio-engineered humans and advanced technology that helped jumpstart "cyberpunk."

**By 2012, Secretary of Defense Leon Panetta was warning that the country could face a "cyber Pearl Harbor."**

## WHEN SCI FI AND REALITY CONVERGED

A year after "Blade Runner," John Badham's box-office success "War Games" hit the cinemas, and fact converged with fiction. In the film a young high school hacker inadvertently infiltrates military computers and almost sets off World War III. While developing the script, screen writers Lawrence Lasker and Walter F. Parkes met with actual cybersecurity experts from Stanford Research Institute and RAND Corporation and talked at length with a young California hacker who was the inspiration for the character played by Matthew Broderick. Was the scenario depicted one that could actually transpire?

That was the question the president of the United States wondered after he watched the movie over a weekend break. Ronald Reagan had always been a movie buff, but on this occasion he didn't want to talk up a movie he liked. He asked his top security people if the story he'd seen could happen. None of them knew the answer, including Gen. John W. Vessey Jr., the chairman of the Joint Chiefs of Staff. When Vessey later confirmed for the president that hacking was, indeed, real and computers everywhere were vulnerable to such attacks, it seems to have been the first time that U.S. government officials learned of such capabilities and vulnerabilities. This knowledge prompted eventual passage of The Computer Fraud and Abuse Act in 1986. During debate about the bill in congressional hearings, clips from "War Games" were shown. Yet, even then there did not appear to be any sense of real urgency about the matter, according to Fred Kaplan in his 2016 book "Dark Territory: The Secret History of Cyberwar." It would not be until Richard Clarke's tenure as presidential advisor to Clinton and Bush more than a decade later that cybersecurity would be taken more seriously.

A year after "War Games" came William Gibson's novel "Neuromancer," in which Gibson coined the term "cyberspace" and imagined a world with hacktivists and computers able to search for and retrieve any information in order to control human beings and let loose mayhem. Fact and fiction would converge once again.

## THE REALITY OF A THREAT

Recognition of the dangers may have been slow, but it has most definitely arrived. In 2012, then-Secretary of Defense Leon Panetta warned the Obama Administration that the United States faced the threat of a "cyber Pearl Harbor," a devastating and sudden attack on the nation's critical infrastructure. In a 2019 interview with journalist Adam Stone from Fifth Domain, Panetta elaborated: "The American people needed to know that the potential for a paralyzing attack was there. We had known that cyberattacks could be used to interrupt business, to gain intellectual property. We knew about hacking. But the fact that a sophisticated virus could be used to virtually paralyze our country, to take down our electric grid, take down our financial systems. . .that potential was there and real."

In the wake of Russia's invasion of Ukraine on February 24, cyberwar appears to be here and real. Even Thomas Rid, the author of "Cyberwar Will Not Take Place," has acknowledged as much. In a recent opinion piece published in The New York Times, he wrote: "Cyberwar has come, is happening now and will most likely escalate. But the digital confrontation is playing out in the shadows, as inconspicuous as it is insidious." Cyberwar and kinetic war have become intertwined, it seems. At this writing, it's impossible to know how the war in Ukraine, and its repercussions, will play out. The one thing that seems safe to say is that no one who works in cybersecurity, or has been paying attention to these developments, should be taking cyberpeace for granted.

## SOURCE TIMELINE

### NONFICTION

#### ACADEMIC SCHOLARSHIP/POLICY & IT CORPORATE REPORTS/ JOURNALISM/DOCUMENTARIES

- 1948 Wiener, Norbert. "Cybernetics"
- 1987 Davies, Owen. "Cyberwars"
- 1992 Der Derian, James. "Antidiplomacy: Spies, Terror, Speed, and War"
- 1993 Arquilla, John, Ronfeldt, David. "Cyberwar is Coming"
- 1998 Denning, Dorothy. "Information Warfare and Security"
- 1999 Qiao Liang and Wang Xiangsui. "Unrestricted Warfare"
- 2001 Denning, Dorothy. "Cyberwarriors: Activists and Terrorists Turn to Cyberspace"
- 2007 Wilson, Clay. "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues"
- 2009 Hansen, Lena, Nissenbaum, Helen. "Digital Disaster, Cybersecurity, and the Copenhagen School"
- 2009 Kurtz, Paul B., DeCarlo, David W. and Simpson, Stacey. "Virtual Criminology Report: Virtually Here: The Age of Cyber Warfare"
- 2010 Clarke, Richard, Knake, Robert. "Cyber War: The Next Threat to National Security and What to Do About It"
- 2010 Cornish, Paul, Livingstone, David, Clemente, Dave and Yorke, Claire. "On Cyber Warfare"
- 2011 Gibney, Alex. "StuxNet: Cyberwar" (Documentary)
- 2012 Arquilla, John. "Cyberwar Is Already Upon Us"
- 2012 Kirsch, Cassandra. "Science Fiction No More: Cyber Warfare and the United States"
- 2012 Rid, Thomas. "Cyber War Will Not Take Place"
- 2013 Garrie, Daniel. "Defining Cyberwarfare...In Hopes of Preventing It" (video)
- 2013 Healey, Jason. "A Fierce Domain: Conflict in Cyberspace, 1986 to 2012"
- 2013 Rosenzweig, Paul. "Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World"
- 2014 Ranger, Steve. "Facing the Threat of a Global Cyber War Changing the World"
- 2014 Richards, Julian. "CYBER WARFARE"
- 2015 Brose, Richard. "Cyber War, Net War, and the Future of Cyberdefense"
- 2015 Vetter, Kim. "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon"
- 2016 Kaplan, Fred. "Dark Territory: The Secret History of Cyberwar"
- 2017 Der Derian, James. "The Cyber Age Demands a New Understanding of War—but We'd Better Hurry"
- 2017 Haizler, Omry. "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking"
- 2018 Bankston, Kevin. "How Sci-Fi Like 'WarGames' Led to Real Policy During the Reagan Administration"
- 2018 Ranger, Steve. "What is Cyberwar? Everything you need to know about the frightening future of digital conflict"
- 2019 Greenberg, Andy. "Sandworm"
- 2019 Greenberg, Andy. "The Wired Guide to Cyberwar"
- 2019 Stone, Adam. "How Leon Panetta's 'Cyber Pearl Harbor' Warning Shaped Cyber Command"
- 2020 Neumann, Peter R.. "Bluster: Donald Trump's War on Terror"
- 2021 Plastic Pills Production. "Cyberwar: The Gulf War Did Not Take Place/Paul Virilio" (video)
- 2022 Ott, Haley. "Information warfare expert says U.S. is finally countering Russia at its own Game"
- 2022 Rid, Thomas. "Why You Haven't Heard About the Secret Cyberwar in Ukraine"

### FICTION

#### MULTIMEDIA/SCI-FI /FANTASY/THRILLERS/VIDEO GAMES

- 1897 Wells, H. G. "The War of the Worlds"
- 1940 Asimov, Isaac. "First books in Robot series"
- 1950 Vonnegut, Jr., Kurt. "EPICAC"
- 1958 Sheckley, Robert. "The Gun Without a Bang"
- 1965 Herbert, Frank. "Dune"
- 1967 Hamner, Robert, Coon, Gene L.. "Star Trek" season 1 episode 23: "A Taste of Armageddon"
- 1968 Dick, Philip K.. "Do Androids Dream of Electric Sheep?"
- 1968 Fontana, D.C.. "Star Trek" season 2 episode 24: "The Ultimate Computer"
- 1968 Kubrick, Stanley. "2001: A Space Odyssey"
- 1977 Lucas, George. "Star War"
- 1982 Scott, Ridley. "Blade Runner"
- 1983 Badham, John. "War Games"
- 1984 Clancy, Tom. "The Hunt for Red October"
- 1984 Gibson, William. "Neuromancer"
- 1999 Stephenson, Neil. "Cryptonomicon"
- 2007 Clarke, Richard. "Breakpoint"
- 2007 Bioware. "Mass Effect" (video game)
- 2012 Clancy, Tom, Greaney, Mark. "Threat Vector"

# WHAT THE INTERNATIONAL LEGAL EXPERTS SAY ABOUT CYBERWAR

AN INTERVIEW WITH BRIGHAM YOUNG UNIVERSITY LAW PROFESSOR **ERIC JENSEN**



Eric Jensen

“When you talk about cyberwarfare, it’s important to make the distinction between cyber activities and those that actually lead to armed conflict.”

*Hello, I’m David Hechler, a writer and editor at TAG Cyber. My guest today is Eric Jensen, a law professor at Brigham Young University in Provo, Utah, who’s an expert on cyberwarfare. His expertise also includes the law of armed conflict, public international law and national security law. Early in his career, Professor Jensen spent 20 years in the United States Army as both a Cavalry officer and a military lawyer. During this time, he taught law and was a legal adviser in places like Iraq, Macedonia and Bosnia. Perhaps most important for the purposes of this discussion, he was one of the international group of experts who created the Tallinn Manual in 2013, and the [Tallinn Manual 2.0](#) in 2017, which presented the authors’ best understanding of the norms and generally accepted rules, as far as they exist, that govern first war and then cyberwar.*

**TAG Cyber:** *When we started planning a special package on cyberwar for our Security Quarterly, we had no idea that Russia was going to invade Ukraine, but here we are. And our conversation will not be limited to history and hypotheticals. When and how did you get particularly interested in cyberwarfare?*

**ERIC JENSEN:** It’s a little bit of serendipity. Back in 2000, I was at the military’s course for midlevel officers who are JAGs [judge advocate generals]—military lawyers—and I was looking for a paper topic. I went into my paper advisor and said, “So what do you think is an

## “The first really big [act of cyberwar] was the malware known as Stuxnet...”

interesting topic that might be coming up in the future?” And he said, “Well, I read this article the other day about something to do with cyber. And that sounded interesting. I don’t know anything about it, but you may want to look into that.” And the rest is history, as they say.

**TAG Cyber: How do you define cyberwarfare?**

**JENSEN:** When you talk about cyberwarfare, it’s important to make the distinction between cyber activities or operations, and those that actually lead to armed conflict. We don’t use, at least in the legal world, that term “warfare” much anymore. We talk more in terms of

armed conflict, but they’re relatively equivalent. So what we think of as war is usually an armed conflict between two nations or states, as we call them in international law, i.e. Russia and Ukraine. And we term that international armed conflict. We also have this term noninternational armed conflict, which means a fight between a state and a nonstate actor like Al-Qaeda or ISIS. So when the United States is in a conflict with Al-Qaeda, that’s a noninternational armed conflict. But in the traditional sense of war, we would probably only refer to these interstate conflicts. For cyberwarfare, we have a good example in Russia’s use of force against Georgia back in the late 2000s. But outside of Russia and Ukraine now, most of the cyber activities that go on are below the threshold of armed conflict—poking, prodding, gathering intelligence, stealing data, stuff like that. And that doesn’t really count as cyberwarfare in the legal sense.

**TAG Cyber: Right now, as I understand it, there is no black letter, international law governing cyberwar.**

**JENSEN:** We who did the Tallinn Manuals, our approach was that there need not be some particular law that just applied to cyber. Instead, cyber tools are like other tools, like bombs, missiles, influence operations, psychological operations, where the existing law doesn’t limit them. Instead, it applies to them. And our job in Tallinn was to say how those laws applied to cyber activities. So I guess my response would be there isn’t, but there needn’t be because in most cases the current law meets those requirements.

**TAG Cyber: So what we’re talking about is norms, understandings, general consensus. Is that a fair assessment?**

**JENSEN:** That’s an absolutely fair assessment. There is certainly some codified law. But the context, the meat of that law is also done by state practice, by what states agree, what they think—consensus, as you say,

**TAG Cyber: I have heard [Microsoft president and chief legal officer] Brad Smith say that there ought to be a digital Geneva Convention. And that’s what’s really missing here. What do you have to say about that?**

**JENSEN:** A couple of my good friends are on the same side and think that this would be helpful. And I think that there might be ways where this would be helpful. There are certainly areas where the international community has not come to consensus on the application of current international law to cyber operations. Like how does the law of sovereignty apply to cyber activities? The United States, for example, takes a very different approach on that than some of its European allies. So there might be usefulness in having a Geneva Convention that highlighted some of these areas where there is still disagreement. My own view is that that’s not necessary. I think, over time, as states interact with each other, as we continue to have discussions like the discussions that are going on in the UN about this, we will come to consensus.



**TAG Cyber:** *To date, do you believe there have been actions by nation-states that were acts of cyberwar, and are generally accepted as such?*

**JENSEN:** Yes. I think there are very few, but there are some that I think crossed that threshold. The first really big one was the malware known as [Stuxnet](#), assuming that it was created by and used by the United States, or Israel, or some combination of them against Iran and its nuclear production facilities. I think that that was probably a use of force as defined in [Article 2\(4\)](#) of the UN Charter, which is what we say is the threshold for war or armed conflict. I think the destructive effects—destroying almost 1000 centrifuges, really setting back Iran’s nuclear production capability—was sufficiently significant to count as a use of force. There have been others since, like Russia’s use of [NotPetya](#) or other viruses against Ukraine back in 2016 and 2017.

**TAG Cyber:** *There are some people who favor a definition of cyberwar that requires there to be casualties, even death, the same way that you would expect in a “kinetic” war. Stuxnet does not qualify on that ground. So your definition does not require that there be casualties. Is this a divide where there are a number of people on one side and a number of people on the other?*

**JENSEN:** I don’t think it’s a huge divide. My definition would certainly include casualties, but it also includes significant civilian damage—so damage to structures and buildings. My sense is that that’s the majority opinion. That’s certainly the opinion that the Tallinn Manuals take. And I think that most governments take. If you think of this in the kinetic world, if someone launched a missile and it landed in the middle of Central Park in New York but didn’t explode, we would still say the United States was the victim of some kind of an attack, even though there was no civilian casualty, right? So in my view, that would be analogous to a cyberassault. If a cyber something does damage, or at least shows intention to do significant damage, then you have to say, “That’s something we ought to contemplate as potentially a use of force.”

**TAG Cyber:** *Let’s talk about the [Russian attack on Georgia in 2008](#), which you alluded to earlier. There were cyberattacks in advance of the kinetic attacks. Were both of those activities acts of war?*

**JENSEN:** I view those initial cyberattacks by the Russian military against Georgia as *in conjunction with* an armed attack. The tanks were already on the border, the military was already massing. And the cyberattacks were really just kind of preparation for the onset of the kinetic attack. So in my view, that’s really the first example not of two separate attacks, but of attacks in conjunction. And I think that’s where we’re going. The current Russia-Ukraine conflict reinforces that. What you’re going to have most often is some kind of a cyberattack in conjunction with the kinetic attack, and in combination they will lead to major conflict.

**TAG Cyber:** *Would you say that Russia’s attack on Ukraine has been comparable to its attack on Georgia?*

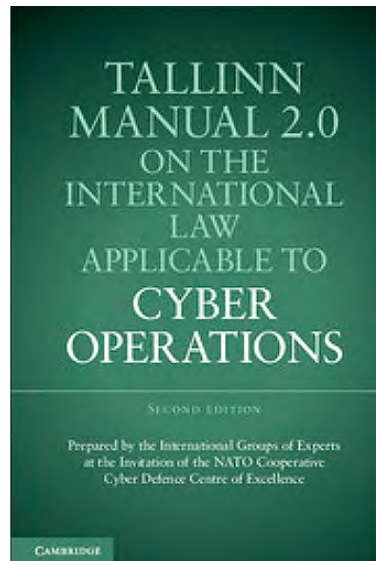
**JENSEN:** I think that Russia’s attack on Georgia was more effective because, of course, Ukraine had been the victim of many Russian cyberattacks prior to this time. And so Ukraine anticipated Russia’s activities more effectively than Georgia had. But from Russia’s perspective, as a matter of tactics and operational approach, I think it was the same.

**TAG Cyber:** *Let’s turn to the Tallinn Manuals. How did you end up in Tallinn, the capital of Estonia, to work on this project? Did you get a phone call in the morning telling you to get on a plane?*

**JENSEN:** It did kind of happen like that. [Michael N. Schmitt](#) is really the brains behind this project. He has been thinking about cyber stuff since before cyber was probably even a word. And he is, in my view, one of the if not *the* world’s expert on the application of cyber law. NATO came to him—the [NATO Cooperative Cyber Defence Centre of Excellence](#) (CCDCOE). After Estonia had had an experience with Russia and Russian hackers or hactivists in 2007, NATO started thinking, “Wow, we ought to really think about what the cyber rules are.” They called Mike Schmitt, knowing he was the smartest guy in the world on this, and said, “Mike, what can we do?” And Mike suggested, “Let’s get some people together

who are law-of-war experts, who are cyber experts from around the world, and get us in a room, and let's write down some rules and see if we can come up with guidance." Mike determined that I was one of those people and gave me a call, and with a bunch of other folks we got together and put together the manuals.

**TAG Cyber: What was it like meeting in this place that had suffered this monthslong attack very early in the cyber world, as we know it?**



**“The United States and other countries have been very clear that if you’re attacking us, we can respond in any way that is lawful.”**

**JENSEN:** It was really cool to be doing this in Estonia, because the genesis for Russia’s interaction with Estonia was the movement of a Russian war memorial from the center of town out to a cemetery. And the cemetery coincidentally happened to be very close to the building that we were meeting in. And so a couple of times, on a break, I would go out and walk to the cemetery, and there was the war memorial. And so it was very real to be doing this there, knowing that this was a nation that had suffered from a **cyber operation** that shut down the banking system, shut down the government system, they had to move some of those services to the U.K. for some period of time to function. And so having it right there gave us all the importance of what we were actually doing.

**TAG Cyber: One of the tricky issues that the manuals had to deal with, and that we all have to deal with, is attribution. Because in certain nation-states, for instance Russia and China, it isn’t always clear whether a group acting at the behest of the state is involved, or the state is unaware or turns a willful blind eye. How did you, the group of experts, deal with that?**

**JENSEN:** This is really important, especially with cyber activities, because cyberhackers will, as a matter of course, try and cloak their identity. They will attack through any number of intermediary systems so that as you’re trying to do the forensics to get back to who actually was the cause of this, it takes you a long time. It’s obscured, you’re not really sure. And they do this because, under international law, if you want to attribute an act to a nation-state, you have to be able to pin it on either an entity of that state like the CIA, or the Department of Defense, or you have to pin it on someone who is acting with the authority of that state. Or you have to depend on someone who that state is exercising control of, and sufficient control that you can attribute it to the state. And this is one of the great hang-ups with cyber. States understand what that level of control is, and they try and provide just under that level of control. So they can say, “Not us. That’s just these hacktivists acting on their own. Sure we’re providing them the cyber tool. Sure we’re providing them potential targets. But we’re not telling them day to day what they need to be doing as they conduct these cyberattacks.” That’s a huge issue and one of those things that these Geneva Convention people argue: “Let’s have a Geneva Convention, because we can clarify attribution in the cyber context.”

**TAG Cyber: What about the whole issue of hacking back? Meaning if a nation-state is attacked, what are its rights and opportunities to take defensive action, even if it requires offensive weapons?**

**JENSEN:** So again, this is a really important and complex question. The same self-defense rules apply. If what is happening to me is the equivalent of an armed attack under Article 51 of the UN Charter, then I can use force in response. And as you implied, that force, even if the hack to me is all cyber, in my response I’m not limited to cyber responses. The United States and other countries have been very

clear that if you're attacking us, we can respond in any way that is lawful. We don't have to respond in kind. The more difficult questions lie with cyber activities that are below attacks. How do we respond to them? And if they do something, for example, that is violative of the state's functions, what we call the **domaine réservé**—things that are inherent to states—and is coercive, then you can respond with countermeasures. Countermeasures are otherwise unlawful acts, so it might be an unlawful cyberattack back, but is made lawful under international law for the purpose of bringing that violating state back into compliance.

**TAG Cyber: You referred to cyber activities “below attacks.” Can you give me examples?**

**JENSEN:** You might remember that there was a movie that was made about the North Korean leader, and the gist was to make light of him. And North Korea conducted cyberattacks—some **cyber activities**, I should say—and threatened more. Well, the U.S. took that as a limitation on freedom of speech, something inherent to our government. And so the U.S. could have responded, and maybe did respond in a way that said to North Korea, through cyber tools, “Don't mess with us because we can mess with you back.” So what North Korea did with their cyber hacks wasn't a use of force. It wasn't an attack, as we would say. But it was still intrusive on our government's capabilities, it was still intrusive on the freedom of speech of our citizens.

**TAG Cyber: I understand that your group made an effort to reach out to the international community and solicit their feedback on what you did. What were the responses?**

**JENSEN:** After the Tallinn Manual 1 and Tallinn Manual 2.0, we told states we wanted their input and we sent drafts out to them.” We told them at the time that we would not disclose their input to the public, but that we would consider their input in our discussions. Many states took advantage of that opportunity. Now, I have to caveat that by saying we didn't automatically incorporate that state input because, as I mentioned earlier, the Tallinn Manual is our opinions, the group of experts, but we certainly were very, very interested in state input. And we're grateful that states were willing to cooperate. The cooperation of states was significantly more for Tallinn 2.0 than Tallinn 1.0, because I think states had a sense, “OK, they will take our input, and they won't spread it all over the world as official statements.”

**TAG Cyber: One thing I found really fascinating about your approach was that you not only laid out what you as a group believed, but when there was internal disagreement, you added into your commentary the scorecard. You said, “Well, we split down the middle.” Why did you do that? And what kind of response have you heard about that approach?**

**JENSEN:** I actually think this is the most valuable part of the manual. There are black letter rules that we all agreed on. Everybody has to agree on every word of the black letter rule. And then below comes all the commentary. So the black letter rule might be that cyber activity that is a use of force is a violation of Article 2(4) of the UN Charter. And then we talk about all the nuances to that, and where we agree and disagree. And for states, that's important, because as they read this, they say, “The black letter law's pretty simple. But what are the options? What are the nuances, what are the tricky parts?” And they have our views, and even see us say, “Look, a third of us thought this, or some of us, or a few of us thought this.”

**TAG Cyber: What contribution do you think these documents made to international law?**

**JENSEN:** People are interested in how the law applies to cyber activities. And I think Tallinn, if it didn't start that discussion, it at least accelerated that discussion. Tallinn Manual 1, of course, only applies to actual war, or armed conflict. Tallinn Manual 2.0 applies to all the rest of that stuff. No states came out before the Tallinn Manuals and said, “We think this.” But since then, lots of states have come out and said, “We think this about this.”

**TAG Cyber: Will there be a Tallinn 3.0?**

**JENSEN:** I think there will be. In fact, I think it's already starting to get put together.

# DEATH TO ESPORONTIA!

ESPORONTIA'S NEIGHBOR IS AMASSING TROOPS ON ITS BORDER. ALTHOUGH TROOPS HAVE NOT CROSSED INTO THE COUNTRY, THE TAKEOVER BEGAN YEARS AGO.

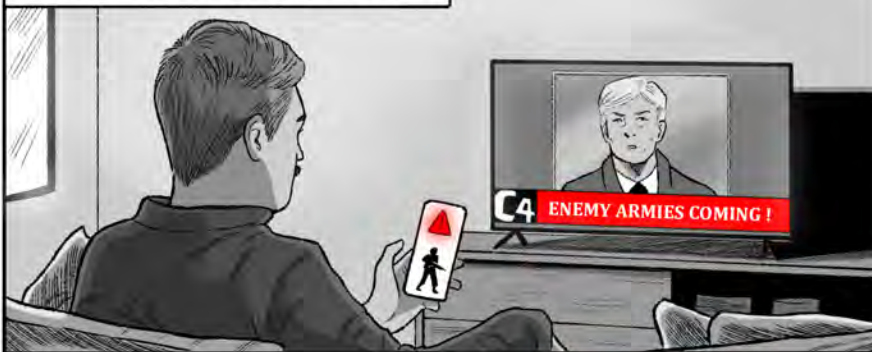
WORDS: CHRIS WILDER & LESTER GOODMAN ART: LUIZ ROSA

## 1. INFORMATION WARFARE

(5-7 YEARS BEFORE THE TAKEOVER)

### FAKE NEWS

RELEASING A CAMPAIGN TO HIGHLIGHT A FAKE THREAT TO THE POPULATION.



### MEDIA MANIPULATION

THE MEDIA IS USED TO REPORT FALSE NARRATIVES.



### DISCORD

DISINFORMATION FOSTERS FRICTION WITHIN THE POPULATION (POLITICIANS, REGIONS, RACES, ETC.)



### REWARDING BAD BEHAVIOR

ENCOURAGING PEOPLE TO GROW DISCORD ORGANICALLY. TURN TRADITIONAL VALUES, PATRIOTISM & TRADITIONS INTO A BAD THING.



### DE-PLATFORMING & CENSORSHIP

SILENCING AND DESTROYING OPPOSING VIEWPOINTS



### RADICALIZATION

SEGMENTING THE PUBLIC INTO "WARRING TRIBES" WHERE EACH TRIBE HAS A COMMON ENEMY AND IS PRONE TO ACT AGAINST THEM MANY TIMES WITH VIOLENCE AND RIOTS.





# 2. ECONOMIC WARFARE

(3-5 YEARS BEFORE THE TAKEOVER)

**FLOOD THE MARKET WITH COUNTERFEIT AND DANGEROUS GOODS ESPECIALLY THOSE NEEDED FOR SURVIVAL, ESPECIALLY PHARMACELTICALS OR DRUGS THAT KILL A CERTAIN PERCENTAGE OF THE POPULATION.**



**DISRUPT TRANSPORT CHANNELS UPSETTING SUPPLY CHAIN INTEGRITY**



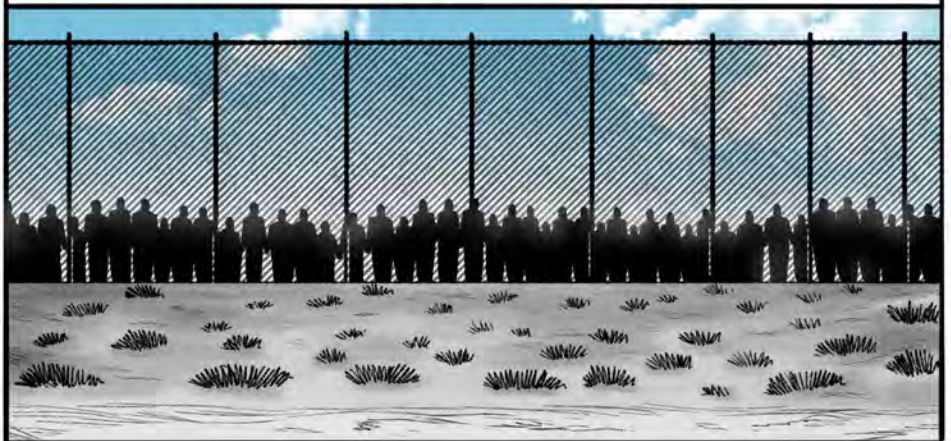
**INITIATE SOCIAL ENGINEERING CYBER ATTACKS AGAINST GOVERNMENT AND THE GENERAL POPULATION TO CREATE FINANCIAL UNCERTAINTY**



**INITIATE SOCIAL ENGINEERING CYBERATTACKS AGAINST TRUSTED INSTITUTIONS AND GOVERNMENT MORE FINANCIAL UNCERTAINTY**



**CREATE A REFUGEE/IMMIGRANT CRISIS (FALSE FLAG INVASION) FLOOD THE BORDER WITH UNSKILLED AND POOR WORKING-CLASS PEOPLE THAT THREATEN THE JOBS AND LIVELIHOODS OF ITS CITIZENS.**

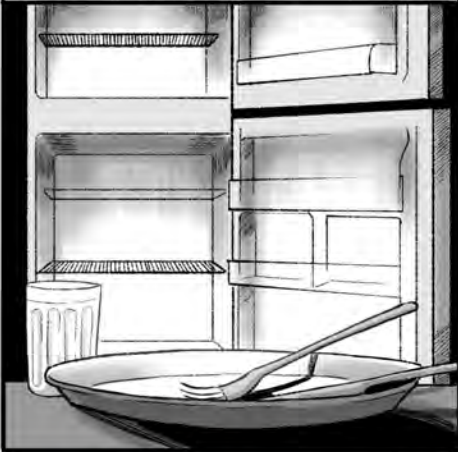




# 3. CYBER WARFARE

(1-2 YEARS BEFORE THE TAKEOVER)

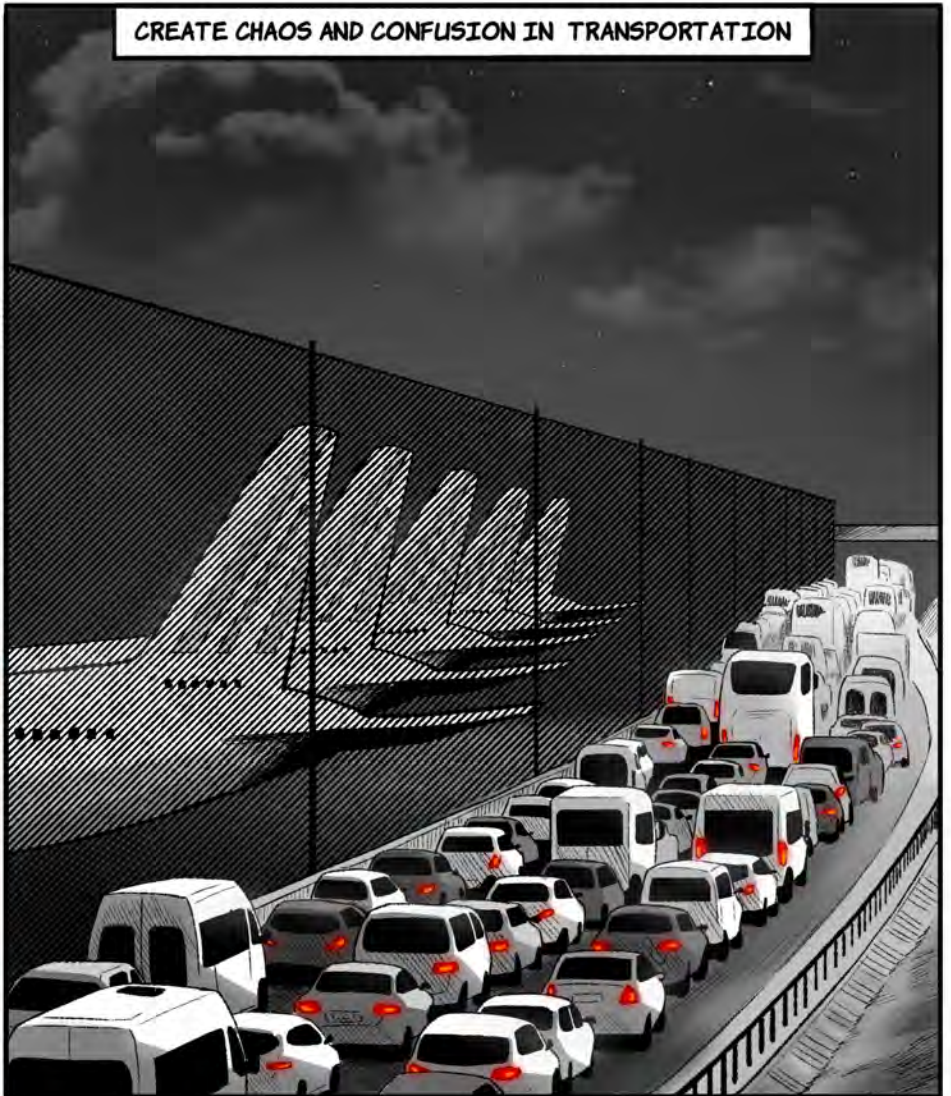
**TAMPER WITH THE FOOD AND WATER SUPPLY**



**CONTROL COMMUNICATIONS**  
TAKEDOWN INTERNET, MOBILE, TELEPHONE, SOCIAL MEDIA



**CREATE CHAOS AND CONFUSION IN TRANSPORTATION**



**ATTACK THE ENERGY GRID**  
TURN OFF THE LIGHTS, SHUT OFF THE GAS, STOP ENERGY PRODUCTION.



**4. REQUIRE FULL SURRENDER WITHOUT FIRING A SHOT**  
(ZERO DAY)



©2022 TAG Cyber

# DEATH TO ESPORONTIA!

(PART II)

CHRISTOPHER R. WILDER

This article provides an example anatomy of a seizure by an aggressor that takes over its neighbor without firing a shot. It describes how bad-actor nation-states architect and execute massive psychological and cybersecurity operations to control the government and citizens of their adversaries.

## PROLOGUE

*The fictional country of Esporontia's neighbor to the north is amassing troops on its border. Although troops have not crossed into the country, the takeover began years ago. Tensions are high, and an invasion seems to be imminent. The steps outlined below have led up to this moment.*

## STEP 1: DISINFORMATION WARFARE (5-7 YEARS BEFORE THE TAKEOVER)

Information warfare (IW) has increased in recent years as the internet and social media have become mainstream. Disinformation warfare uses false information, propaganda and hoaxes to disrupt an opponent's operations and credibility. Its goal is to demoralize and divide the population, politics and military, and to damage an opponent's image globally.

Disinformation consists of many strategies used to disrupt a bad actor's opponents. For example:

### Create Discord and Establish the Narrative

**1. Fake News**—Advisories plant and use false or "fake" news on social media and fraudulent news websites, generating a counternarrative that creates doubt, division and discord.

**2. Social Media Bots**—Arguably, social media bots pose the largest threat to naive users during a disinformation campaign. Bad actors use bots to falsely amplify a person, company, campaign or candidate's popularity or artificially impact a stock, company or social movement. For example, social media bots can influence elections, manipulate financial markets, amplify phishing and malware attacks, spread misinformation spam and push down free speech.

**3. Media Manipulation**—Bad actors will use the media to falsely portray Esporontia as the true aggressors. Unchecked, many mainstream news organizations will gleefully follow the herd mentality and report a false narrative, thereby justifying the bad actor's provocative actions.

#### 4. Applying Artificial Intelligence (AI) to Create Chaos—

Deepfake is how bad actors use AI to simulate and distort reality: by distributing AI-generated computer imagery to replace one person's likeness with another in recorded videos or other media. Nation-states and bad actors use deepfake to create a misleading narrative to change a political or war stance context or campaign, or potentially start a war. Deepfakes raise concerns about a country's economy or the government itself. Deploying deepfake is a deliberate means of deceiving and appeasing the population into compliance. Recently, deepfake has become a key component of cyberoperations. They manipulate information for deceptive purposes and are now key assets for psychological warfare operations.

*"In warfare, if you control the narrative, you control the population."*

*—Christopher R. Wilder*

### CREATE DISCORD AND IDENTIFY A COMMON ENEMY FROM WITHIN

Bad-actor nation-states use psychological operations (PsyOps) to achieve their goals. This stage uses disinformation and tactics to reduce trust and increase friction between politicians, communities, regions, races, wealth, immigrants/refugees, businesses, religions, etc. The most successful campaigns focus on an aligned threat, including:

**1. Rewarding Bad Behavior**—Encouraging people to find validation and approval for uncharismatic or "traditional" values. Acts of patriotism are met with disinformation campaigns and a willing media to alter behavior among the population to grow discord organically. They turn traditional values, patriotism and freedom into bad things against the "norms" of what they consider civil. The end goal is to divide the Esporontia population into warring tribes that are easily manipulated for political and social benefit.

**2. Deplatforming, Censorship and Radicalization**—Attempting to silence and destroy opposing viewpoints not held by the establishment (or whatever is deemed moral authority). I have worked with multiple individuals for several years to understand how people become radicalized to a specific ideology. My journey has led me to work with the **Change Minds** team. These individuals included the late Jesse Morton, former al-Qaida recruiter and propagandist who was captured and turned, and who eventually dedicated his life to preventing and countering violent extremism; Daryl Davis, a black musician who built a network of communication and trust with over 200 members of the Ku Klux Klan to "remove their hoods and permanently leave the Klan"; and Bill Ottman, founder and CEO of **Minds**, a blockchain, open source, community-based, antithetical-to-Facebook social media platform focused on privacy and free speech.

Change Minds contends that there are many unintended consequences when it comes to censorship. For example, the Brookings Institution stated that censoring the social media accounts of ISIS and other caliphate members directly led to the rise of extremism and the movement's rise in the Middle East. The deplatforming of dissenting voices encourages radicalism. Social engineering, deplatforming and censorship speed up the process and effectively raise the intensity of radicalization by taking away the voice of common citizens while pushing them to a specific and harmful dogma.

**3. Influence and Voices in a Vacuum**—Segmenting the public into "warring tribes," where each tribe has a common enemy, while at the same time censoring and muting alternative voices. This creates a vacuum and an environment for a naive and easily manipulated population to act against a common enemy, violently. Although effective in the short term, this strategy is not sustainable.



## STEP 2: ECONOMIC WARFARE (3–5 YEARS BEFORE THE TAKEOVER)

Economic warfare is used to diminish a country's natural resources exports and establish bad consumer behavior. Bad actors and criminals will develop platforms to introduce counterfeit goods, disrupt legit supply chains and attack trusted institutions like law enforcement and medical. For example, aggressive actors will attempt to disrupt traditional industries to cause distrust and interrupt how goods are transported.

*“It's easier to fool people than to convince them that they have been fooled.”*

*—Mark Twain*

### **1. Flood the market with counterfeit and dangerous goods—**

Experts estimate that counterfeit goods worldwide are over \$520 billion and account for nearly 3 percent of the global economy. Counterfeit rings have continued to be bolder and more sophisticated, especially during the pandemic.

To affect the economy, bad actors work directly with originating factories (mostly based in Eastern Europe and Southwest Asia) to “white label” an identical product. From there, the bad actors set up companies to purchase the newly labeled products and filter the proceeds through preferred jurisdictions like the Seychelles, Jordan, Panama, etc.—countries that are light on knowing your customer (KYC) constraints. Once these networks are established, bad-actor nations are ready to sell counterfeit goods worldwide, thereby taking away the country's ability to compete with authentic goods and services in the global market.

Bad actors will leverage a combination of online and offline channels to influence customer behavior. These channels provide cheap, easy access to counterfeit products while eroding the trust of established brands and increasing the legitimacy of new off-brand or fake products.

**2. Disrupt transport channels (sea, air, land, communications, R&D, etc.)—**Bad actors rely on disinformation to influence geographical, sociopolitical and socioeconomic climates to affect a government's supply chain dynamics. For example, almost 80 percent of the world's active pharmaceutical ingredients (API) come from China or India. Bad actors understand that if they disrupt transport channels (land, sea, air), criminals can cause individuals, governments and organizations to question the integrity of the supply chain. For example, a disruption in manufacturing vaccines and pharmaceutical plants can raise concerns about its FDA quality systems approach (FQSA) or ICH-Q10 standards—forcing legitimate companies to deal with chaos in their supply chains. The desired effect of bad actors is to have countries panic over a diminished supply and come in at the online and local level with both genuine and counterfeit products to ensure supply chain integrity.

**3. Initiate sophisticated social engineering cyberattacks against trusted institutions, the government and the population—**Social engineering is a process that uses psychological tactics and manipulation to trick a population into making security mistakes that give away their personal or their organization's sensitive information. Social engineering has four pillars in its life cycle: identifying the “marks”; hooking the marks; executing the scheme; and exiting without arousing suspicion. Successful social engineering attacks create doubt, distrust and discord across companies, organizations and governments. Social engineering is a good way for nation-states to exploit the secrets, financial information and personal data of unsuspecting individuals. The stages of social engineering include:

#### **Stage 1: Identifying the Marks**

1. Identify and profile the intended victims.
2. Initiate surveillance, backgrounds and intelligence on the targets.
3. Determine the most appropriate attack methods.

## Stage 2: Hooking the Marks

1. Engage and interact with the intended victims.
2. Create the narrative and spin the story.
3. Take control of the narrative and establish dominance.

## Stage 3: Executing the Scheme

1. Expand the foothold by demonstrating trust and reliability.
2. Execute the attack.
3. Extract the information and use user intelligence to disrupt the business or agency.

## Stage 4: Exiting

1. Remove the evidence of a malicious attack or data compromise.
2. Cover your tracks.
3. Leave the mark without a trace and bring the charade to a natural end.

**4. Create a refugee/immigrant crisis (false flag invasion)**—One of the most divisive political issues is immigration. Attackers will flood the border with unskilled and poor working-class people and criminals who threaten the jobs, safety and livelihoods of the country's citizens. Sadly, countries often use immigration to foster political and structural changes as a wedge issue before a takeover.

False flag attacks/invasions are political or military actions to blame an opponent for starting a conflict. Nations often "flood the border" with desperate refugees and conduct simulated attacks on themselves to blame the enemy as a pretext for going to war. False flags were first used in the 16th century by pirates flying the flag of a friendly nation to deceive merchant ships into allowing them to come near. Today, false flag invasions are deployed along disputed borders to provoke military conflicts.

## STEP 3: CYBERWARFARE (1-2 YEARS BEFORE THE TAKEOVER)

The volume, sophistication and severity of cyberattacks demonstrate the inevitability of organizations and governments no longer asking if they are vulnerable; rather, it's when and how the breach will occur. The attack surface has expanded exponentially. Realizing that the network perimeter is rapidly diminishing because of the cloud, the internet of things (IoT) and edge computing, organizations and agencies acknowledge that the security battlefield is playing out inside AND outside their infrastructure and networks. Sadly, most countries lack the expertise to ward off sophisticated advanced persistent threats (APT) and do not have the trained personnel or the security controls to defend against new and evolving zero-day threats.

To quickly take over a country, adversaries must disrupt the lives of the targeted population. Once bad actors control the networks and infrastructure, they can demoralize the people into submission and be liberators by restoring everyday conveniences; however, they must first demonstrate their ability to take essentials away.

**1. Disrupt and tamper with the food and water supply**—Denying food and water creates a desperate and weak population. Bad actors can effectively destroy morale and the country if the people cannot access food and water. A hungry nation is a weak nation, and the government is, in most cases, to blame.

**2. Keep the population uneducated, uninformed and illiterate by disrupting networks and communications**—A uninformed and illiterate population is easy to manipulate. Bad actors have an easy time recruiting illiterate followers into their ranks. In my time with the intelligence community (IC),

*"A house divided against itself cannot stand."*

*—President Abraham Lincoln*



we used these people to be our eyes and ears, provide intelligence and destroy unity while building loyalty in a community from the inside out. This is sometimes called a “rat-chain.”

**3. Control communications throughout the population**—Once you control the population’s information and communications, it is easy to influence their ranks. Bad actors will initiate campaigns to poison their ideologies, customs, traditions and identity, and tear communities and people apart using psychological, communications, and social media against the population. Communities will eventually argue over trivial things or quickly label their friends and neighbors as racists, misogynists, traitors and even Luddites or troglodytes. It is cruel but effective.

In one of the most important steps to controlling the narrative, intruding forces will shut down cellular communications, the internet and social media platforms to stop the population from communicating and coordinating to form an insurgency or resistance.

**4. Attack the energy grid**—Turn off the lights, shut off the gas, stop energy production. Bad actors train and equip students to carry out proactive cyber actions on behalf of their government. For example, they challenge their Ph.D. students to develop a thesis on how they would use a cyber-attack on the country’s electrical power grid to cause the most damage, then use a highly trained military cyber offense to execute each attack method. Sadly, there are always a few key points of attack in most county’s power grids where hackers and crackers can cause the most destruction.

**5. Take away everyday conveniences**—Aggressors will take away basic conveniences like energy, HVAC, internet, TV, water and—most importantly to today’s generation—social media to disrupt citizens’ lives. In addition, sophisticated bad actors use global resources such as food and fuel to inflate prices and artificially tax the working class. When people pay more for gas, they are less apt to go out to purchase groceries and consumer goods or travel, but more importantly, they are more inclined to blame their government for their woes. Economic false flags are just as effective as false military flags. Sadly, everyone loses.

**6. Create confusion and chaos in transportation**—Shut down electric vehicles, create chaos within traffic patterns and stop public commuter options. For example, if most of the population uses Google and Apple Pay for online payments, and Google and Apple stop accepting payments, this effectively shuts down transportation options and leaves civilians stranded, because they can’t pay for public transit. These disruptions create significant discord and anger among the population, regardless of the aggressor. This is just one example of a real-world blueprint for creating chaos and confusion in transportation during the fog of war.

“A house divided against itself cannot stand.”—President Abraham Lincoln

## STEP 4: REQUIRE FULL SURRENDER WITHOUT FIRING A SHOT (ZERO DAY)

The threat of a ground invasion is daunting and a distraction from the behind-the-scenes activities conducted by the aggressors. Bad-actor nation-states use disinformation, cyberattacks and false flags to bend governments to their will. Bad actors can manipulate a targeted population into compliance by taking away daily essentials and conveniences.

Politicians are interested in remaining in power; the rich and billionaire class focuses on wealth retention; and the general population wants to live normal lives. Aggressors will promise to reinstate all the above in exchange for

*“The greatest victory is that which requires no battle.”*

—Sun Tzu

control over autonomy, security over freedom and comfort over isolation.

The aggressor nation-states will restore their version of liberty and safety in exchange for 1) allegiance to the aggressing country; 2) protection from retaliation from other countries; 3) acknowledgment by the global community of the bad actor's sovereignty and territory; and 4) commitment to establish, expand and engage in trade relationships with the new "entity." Unfortunately, and in most cases, the politicians, the rich, and especially the working class will fall in line and submit to their new overlords. The population chooses security over liberty. You get what you paid for, and bad actors made it happen without firing a shot.

***“Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.”***

***—Benjamin Franklin***





# CYBERWAR...THE DAY AFTER

GARY MCALUM

When I first entered the Air Force as a young second lieutenant in 1983, my first assignment was Castle Air Force Base in California. It was the primary base where they trained B-52 bomber and KC-135 tanker pilots. Those were the golden years of the Cold War, so the possibility of a nuclear conflict with the Soviet Union wasn't out of the realm of possibility. In that very same year, I gathered together one Sunday with several of my Air Force colleagues and watched the movie "The Day After." It was a very dark movie that was based on a fictional war between NATO forces and Warsaw Pact countries that rapidly escalated into a full-scale nuclear exchange between the United States and the Soviet Union. As you can imagine, it was filled with graphic, inconceivable consequences of such a war. I had a hard time sleeping for a while after watching it.

The geopolitical context for that movie I watched nearly 40 years ago feels a lot like what is happening today in Ukraine. And not just in Ukraine—in the South China Sea, in the Middle East and in North Korea. There are many flashpoint scenarios that could lead to nation state conflict on a scale we have not seen before. Recently in Ukraine, we've seen the unprecedented use of advanced hypersonic weapons by Russia even as Vladimir Putin raised the alert level of his nuclear forces. And North Korean dictator Kim Jong-un recently resumed testing of intercontinental ballistic missiles (ICBMs). We are living in precarious times indeed.

Many observers believe that in the next major conflict, cyberwarfare will be a key capability employed by our adversary at a level of scale and intensity we have not seen before. It's something that our military planners worry about. There are also some people who believe that the use of cyberwarfare capabilities by our potential adversaries will be limited—surgically precise and easily controlled. I am not one of those. In fact, I happen to believe the cyber component will create devastating impacts across our nation, impacting not just military systems but many critical infrastructures and daily conveniences we take for granted.



**“Many observers believe that in the next major conflict, cyber warfare will be a key capability employed by our adversary at a level of scale and intensity we have not seen before. It’s something that our military planners worry about.”**

As a former military cyber officer and private sector chief security officer, I have spent many years fighting the cyber fight and planning for worst-case scenarios. The very nature of cyberattacks is unpredictability, but here’s what I think a nation state cyber conflict will look like.

While the initial event will likely involve military or warfighting systems, the cyber component will rapidly come into play. In a true nation state head-to-head confrontation that quickly devolves into significant military kinetic actions, I believe the cycle of escalation will increase rapidly and the cyber aspect will become much more visible. What will that look like in a major conflict? Planes will be shot down, ships blown up, communication and navigation satellites attacked with anti-satellite weapons and human life will be lost at a pace and scale we haven’t seen since WWII. And cyberattacks will be widespread and devastating.

As any military strategist would argue, we can’t know exactly how a true cyberwar will play out because there are scenarios ranging from low-end, inconvenient attacks all the way to the worst-case scenario of unconstrained cyberwarfare. No one knows what that looks like, but I think

there are likely three simultaneous or overlapping scripts that we can expect to deal with. Remember, on the spectrum of possibilities, I’m talking about a far-right scenario where a sophisticated nation state adversary unleashes full cyber power, most likely in conjunction with traditional military kinetic capabilities. It’s a horrible prospect to contemplate, but ignoring the possibility is dangerous.

## **1. DESTRUCTIVE MALWARE**

Destructive malware will be widespread and targeted against military and civilian support systems, government organizations, financial systems and various critical infrastructures. Imagine a Sony Pictures scenario involving large financial institutions, our power infrastructure, and even logistics and transportation systems. It took months for Sony Pictures to fully recover. Can you picture banks or the market being down for just a few days, let alone weeks? And we’ve seen indications of this destructive aspect playing out in recent times.

It was less than five years ago that Russia unleashed NotPetya, a cyberattack targeting Ukrainian power, transportation and financial systems in an attempt to further destabilize the country. But rather than being the cyber equivalent of a precision smart bomb, NotPetya spread rapidly across the globe. That was a relatively unsophisticated attack compared to what a true sophisticated, destructive attack could do if fully unleashed. As of this writing, data wiping malware has already been discovered in Ukraine. So far, researchers have detected new destructive malware—HermeticWiper—on machines in Ukraine and nearby countries Latvia and Lithuania. The wiper abuses legitimate drivers from EaseUS Partition Master software to corrupt data.

## **2. SUSTAINED DISRUPTION OF SERVICES**

Besides destructive attacks, we will have to deal with widespread and sustained disruption of services that we use on a daily basis. But isn’t a distributed denial of service (DDoS) attack easily dealt with? Maybe not. Just last year, the New Zealand Stock exchange experienced a devastating DDoS attack

**“There are also some people who believe that the use of cyber warfare capabilities by our potential adversaries will be limited—surgically precise and easily controlled. I am not one of those.”**



perpetrated by actors demanding a large sum of virtual currency in what became a “ransom denial of service attack” situation. Despite their best efforts to restore and sustain services, exchange trading at NZX was stopped for four days, with “only intermittent periods of availability,” according to a government review. DDoS attacks are not new, and dealing with them should be relatively straightforward. But they have evolved and are easy to execute compared to more sophisticated attacks thanks to the explosive growth of internet-connected devices.

Disruptive attacks can also take the form of widespread delivery of ransomware. Think Colonial Pipeline. We can expect the Colonial Pipeline scenario to play out over and over across many industries and sectors should we be in a major military conflict. And don’t forget the WannaCry ransomware virus back in 2017. WannaCry rampaged across the internet, attacking computers in 150 countries, causing massive productivity losses as businesses, hospitals and government organizations were

forced to rebuild systems from scratch. Ultimately, hundreds of thousands of computers worldwide were affected. Just try to imagine multiple WannaCry viruses unleashed against the digital community. Any sophisticated, nation state actor will certainly use the DDoS and ransomware arrows in its quiver and do it at scale. Imagine the disruption of ATM functions or 911 phone operations or gas station operations or medical services for days and weeks on end.

While the disruptive effects of widespread and sustained DDoS and ransomware attacks are staggering to consider, there is one other aspect of a cyberwar that will likely come into the play, and it doesn’t necessarily fit the context of cyberattacks we’ve been considering. The vulnerability of the world’s transoceanic undersea cable infrastructure is amazingly underestimated, but definitely top of mind for military planners and our potential adversaries.

According to a 2021 article by the Center for Strategic and International Studies (CSIS), these major cable routes are sometimes described as the “world’s information super-highways” and they carry over 95 percent of international data. In comparison with satellites, subsea cables provide high capacity, cost-effective and reliable connections that are critical for our daily lives. There are more than 400 active cables worldwide covering 1.3 million kilometers (half a million miles). Undersea cables make instant communications possible, transporting the vast majority of the data and voice traffic that crosses international boundaries. They also form the backbone of the global economy—roughly \$10 trillion in financial transactions are transmitted via these cables each day.

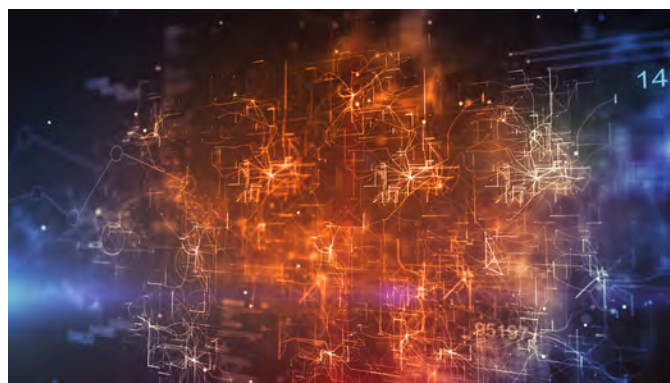
While regional availability of the internet might continue to be accessible if international cables were cut, many critical services rely on data centers that are overseas, particularly the big tech companies based in the U.S. that dominate the web. A company’s data may be housed in a data center located just down the road, but the business application that processes it may be running on a server on another continent. I have personal experience from my military days in dealing with a major communications outage caused by a fishing trawler dragging an anchor across a major undersea cable route. (At least that was the official explanation that was offered.) It made me realize that the potential implications for cyberwar are staggering, and the global undersea infrastructure would be a major target.

### 3. ZERO DAY EXPLOITS

Perhaps the most concerning characteristic of a worst-case cyberwar will be the unconstrained use of zero day exploits creating both destructive effects as well as mass confusion. Think Stuxnet multiple times over. In that case, it was a very sophisticated worm exploit leveraging multiple unknown vulnerabilities in the Microsoft operating system to successfully target SCADA systems supporting Iran's nuclear program, specifically the gas centrifuges used for separating nuclear material. Stuxnet was able to stealthily change the physical performance of the centrifuge system while not allowing the monitoring system to report the anomalies that were injected into the processing. By the time lab personnel discovered the issues, about one fifth of Iran's nuclear centrifuges had been destroyed.

There's no doubt the world's cyber players are stockpiling zero day vulnerabilities and developing sophisticated exploits. If it comes to the worst-case scenario, the U.S. will have to deal with many such complex cyber events. Try to imagine, for example, what would happen if the nation's air traffic control system were compromised in such a way that controllers could not trust what they were seeing on their displays. And then imagine that the same thing happened in power distribution facilities, or water processing plants, or hydro-electric facilities and so on. The possibilities are endless and terrifying.

Some may argue that we've already been involved in a cyber conflict, and there certainly have been plenty of examples of limited cyberwar-like events. I think back to 2007 and the infamous "Web War I" Russian attacks against websites in Estonia, including its parliament, banks and government agencies. Most of the attacks that had any influence on the general population were good old-fashioned DDoS attacks, ranging from single individuals using various methods like ping floods to bigger botnet attacks. During my last military assignment, I recall meeting a senior Estonian official who told me that the attacks themselves were disruptive but not catastrophic. However, he went on to say that the biggest impact was the "loss of confidence in the government" among the people. Ultimately, that very result—a permanent loss of confidence in our government's ability to protect us—could be the lasting effect after a major conflict involving unconstrained cyberwar. And that might spawn a world not so different from the one I found so depressing in "The Day After."





# THE FOUNDER OF A CYBERWAR JOURNAL TALKS ABOUT UKRAINE (AND MORE)

DAVID HECHLER



Daniel Garrie

Daniel Garrie is an unusual lawyer. Or maybe I should say that Daniel Garrie is an unusual tech entrepreneur. Or JAMS mediator. Or journal editor. Or... You get the idea. He has a multifarious background and career, which is uncommon in the worlds of law

and cybersecurity. That was one reason he was a good person to interview right now. The other was that the publication he founded is called the **“Journal of Law and Cyber Warfare.”**

When I contacted him in mid-February to arrange a conversation, neither one of us could have known that the topic would be on everyone’s front burner a month later. But I had a few questions, and he had lots of answers—not limited to the main topic. In addition to editing the journal, which usually comes out biannually, he teaches and writes on this subject. And there were widespread expectations that Vladimir Putin had a detailed lesson plan he was about to unveil in Ukraine and beyond (though many observers, as of this writing, have been surprised that the cyberattacks tentatively attributed to Russia have not been more numerous and effective).

I asked Garrie for an example of cyberwar.

“International law is very complicated,” he began. (It was a statement he would repeat often). “Cyberwar, in my opinion, will always be brought alongside real war. I don’t think you’re going to have cyberwar as a standalone theater of operation. That’s fictionalized, romanticized, TV-induced.”

**“I don’t think you’re going to have cyberwar as a standalone theater of operation. That’s fictionalized, romanticized, TV-induced.”**

The example of cyberwar he presented was Russia's invasion of Georgia in 2008. "They went into Georgia, they ran a massive cyber operation," he said. "They ran their troops shotgun through that country. They hijacked territory. The only difference is the people didn't fight back. What's happening today is that people realize enough's enough."

**"Sometimes talking about wars abroad can focus attention on problems at home."**

A moment later he noted one additional difference. "In the theater of international laws, determined by norms and consensus, there's a lot more consensus and focus today on what's happening in Ukraine than what happened in Georgia. Why that is I can't tell you, but I would say that the global political landscape shifted."

Garrie would like to think that he had something to do with that. For the past decade his publication has sought to fill the void. When he started, "there was nothing," he said. The people who were addressing the issues were largely academics. Very few individuals or companies had experienced anything resembling cyberwar, he said. With the exception, he added, of the financial services industry. Dozens of banks, including JPMorgan Chase, Capital One, PNC Banks and Bank of America weathered 18 months of distributed denial of service attacks that were allegedly launched by **Iranian hackers**, beginning in 2011. But no one seemed to be learning from those experiences. "There was no guidance," Garrie said, "no thought or conversation." (Except inside the U.S. Department of Justice, which in 2016 indicted seven men it deemed responsible for the attacks at the behest of the Iranian government.)

Garrie saw little interest from the broader private sector, even though about 85% of the nation's critical infrastructure is privately owned. He approached U.S. representatives and senators, "and I realized this was not on their radar either." So he decided there was a need. "That's how the Journal came to be," he said. And from the outset it's had one mission. "I wanted to create a balanced journal that wasn't pushing anybody. We're not trying to get business. We're not trying to grow anything. We're simply trying to educate decision-makers across the spectrum."

## **A DIVERSE BACKGROUND**

Garrie was a techie before he earned his law degree. In college he majored in computer engineering and went on to complete his master's in computer science. Before that, he was already infected with the business bug. He co-founded his first startup before he even started college. The startup he settled down with was the one he founded in 2008, three years after he finished law school. It's called **Law and Forensics**, and it's a legal engineering firm that focuses on cybersecurity, computer forensics, data breaches and more. Garrie is also a so-called neutral at JAMS (formerly Judicial Arbitration and Mediation Services) and helps resolve electronic discovery and other disputes around the globe.

He frequently sees himself at the intersection of law and technology—or, more specifically, lawyers and CISOs. When I asked what he wanted his journal to accomplish, he was quick to answer. "Educating people from different perspectives of the legal business," he said. "There's a litany of risks, but very few materials for a CISO to get that are neutral, that are objective," he continued. "People try to dumb it down, make it less complicated. People try to abstract things. And I think that deprives the chief security officers and then the lawyers and cyber professionals, and then insurance executives and business executives from understanding how things work." He paused for a moment. "I mean unfortunately, it's very complicated."

How complicated? He talked about the challenges of advising a company during a crisis. Say there's a demand for a ransomware payment, "and it's associated with a state actor," he said. "Will your

insurance carrier reimburse it?” And does the company have a choice? Philosophical debates are sometimes beside the point, he noted. “Our clients need to operate a business and make money. So what we need to know is are there people we’re going to pay? Are they terrorists? Are they involved in war crimes? Are they associated with a government entity that’s on a no-fly list?”

There’s an even more granular level. “The CISO’s focus is managing the incident, which includes reporting it to the company’s lawyers and management.” Sometimes companies have cybersecurity lawyers. Sometimes Garrie’s company, Law and Forensics, will help them pick lawyers and an incident response firm. “And we help put it all together. I mean, what is the right course of action? Our sole focus is protecting the interests of the company while following the law.”

## BOILING DOWN THE ISSUES

Some of the issues the experts are puzzling over strike Garrie as far less complicated. When I asked if he was surprised that, as far as we know, Russia did not pave the way for its invasion of Ukraine with the kind of robust cyberattacks that some experts expected, Garrie had a quick response. “I’m not surprised,” he said. “They’re using missiles. Those are a lot more effective.”

During the remainder of our conversation, Garrie covered a lot of ground. One subject he dwelled on at length was the importance of public-private partnerships to bulk up cybersecurity. He particularly praised the jobs that [Jen Easterly](#), director of the Cybersecurity and Infrastructure Security Agency (CISA), and [Chris Inglis](#), the White House’s national cyber director, are doing. They’re improving communication and organization within the government, he said. And they’re reaching out to facilitate the flow of information with the private sector. Beyond that, he added, “They’re holding agency heads accountable for bad security hygiene.”

There was one issue he’d touched on earlier that he returned to as we wrapped up. It reminded me of a [conversation](#) I had two years ago with Richard Magnan. Magnan was the general counsel and CISO of a company called Rising Tide, which runs two charitable foundations in Switzerland. As the dual role Magnan played suggested, he, too, had a background in law and tech. And he recognized the need for companies to employ professionals who could bridge the divide between the two.

Like Garrie, Magnan also teaches. He told me about classes designed to help lawyers learn enough about technology to be proficient in their in-house jobs. His students were intelligent enough, but they struggled to learn the basics. In his opinion, this is a widespread problem. On average, lawyers do not have a sufficient grasp of technology to partner effectively with their IT departments to ensure that their companies comply with the law.

At the end of my interview with Garrie, he brought up the same topic. A CISO can be “the best thing since sliced bread,” he said, “but they’re not an expert in international law. They’re good at securing things and managing risk.” He worried about the “communication gap” between CISOs and lawyers. “There needs to be a much more valiant effort,” he went on. “And I know lawyers won’t like this, because it’ll eat into their revenue streams, but they need to educate the CISOs so they can be more effective participants in explaining—or asking the right questions of their legal team. And the legal team needs to ask the right questions of the CISOs so they can properly advise them.”

What it comes down to is that both groups, he said, need to ask a lot more questions. “I still learn new law every day,” he added. “I’m never going to pretend to know everything. But I know how to ask the right questions.” That’s what’s too often missing. “And I really think that’s the reason why a lot of these cyber issues and conflicts arise.”

Sometimes talking about wars abroad can focus attention on problems at home.

# CYBERSECURITY TOOL PORTFOLIO—FRIEND OR FOE?

JENNIFER BAYUK

For those not familiar with the remarkable story of Pegasus, the idea that a cybersecurity tool designed to bolster a nation’s defenses can morph into an offensive cyberweapon may seem daft. Pegasus was first marketed as a surveillance tool designed and proven to provide intelligence with which to find fugitives from justice, thwart terrorist plots, fight organized crime and take down child pornography rings. It provided the intelligence by exploiting vulnerable phones of its targets. Its use was therefore considered in line with wiretaps and other monitoring devices available to law enforcement, at least by the U.S., until it became astonishingly clear that it was used to unjustly hunt nonviolent opponents. The most egregious example of its misuse culminated in the killing of the Washington Post columnist Jamal Khashoggi by Saudi Arabia. The company that produces Pegasus is now on the U.S. Commerce Department’s list of cyberwarfare companies to which U.S. suppliers are prohibited from peddling.

As ironic as it seems, there is a thin line between even business-grade commercial cybersecurity tools and cyberweapons. Like a gun, a cybersecurity tool is not “good” or “bad” in itself, though it may be classified as such, depending on how a given operator uses it.

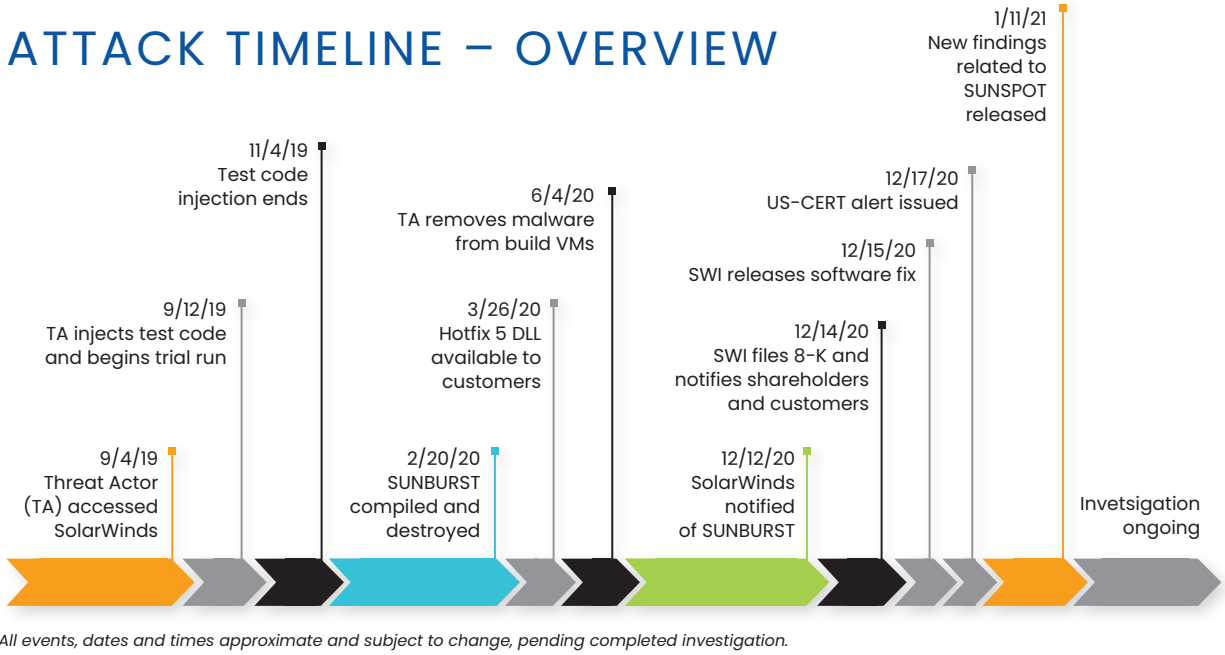
## AN EXEMPLAR CASE STUDY

Another good example comes from the Solorigate case. SolarWinds is a widely used network monitoring tool. Though not designed as a cybersecurity tool, it can provide flow that can be used for network security analysis. Hackers designed a malware payload to exploit a vulnerability in a Microsoft security feature and packaged it within a SolarWinds software release. Using permissions granted by the SolarWinds customer (“victim”) to run SolarWinds’s software, the malware gained access to the victim’s Microsoft authentication token signing certificate and forged access tokens that impersonated the victim’s users and administrators. As is evident in the timeline in Figure 1, attackers were in

**“Like a gun, a cybersecurity tool is not ‘good’ or ‘bad’ in itself, though it may be classified as such, depending on how a given operator uses it.”**



the SolarWinds network, inconspicuously observing and testing malicious software for over four months before deploying it. It has also been reported that the same Microsoft attack vector in the SolarWinds package had been documented in the past, so with hindsight, it is thought to have been used prior to Solorigate. If so, this makes Solorigate a good example of the evolution of cyberweponry. In the hands of one attacker, a difficult-to-perform exploit causes concern. In the hands of a nation-state with virtually unlimited technology resources, it is a matter of time before its full potential is unleashed.



**Figure 1. Solorigate Hack Timeline**

Although it is increasingly obvious that technology products and services can be used as both friend and foe, we have not seen a huge uptake in breach and attack simulation (BAS) on this front. It seems to be left to supplier risk management processes to sound the alarm. While many enterprises are systematically ticking off patterns using targets from the MITRE framework, not many have as systematically created BAS scenarios that assume insider access and threats to their own security tools. So we took a look at the TAG Taxonomy, with the objective of highlighting the most obvious cybersecurity tools that can be turned to foe, and review some abuse cases.

### ENDPOINT SECURITY

In the early days of endpoint security tools, the focus was on security configuration change control and anomaly detection. It was assumed that the remedy for any identified threats was to change the security configuration to prevent further recurrence of the same incident, as well as to test and deploy the new configuration via a highly controlled process. Unfortunately, the ubiquity of the Microsoft desktop in combination with the promiscuous behavior of users made it impossible to control the entry of malicious software using operating system security, and more proactive tools began to emerge. The tools had the ability to quarantine software that appeared to overlap in bits and/or behavior consistent with software known to be malicious. Security professionals at the time were (and still are) peppered with requests for legitimate business software to be let out of quarantine. Now we have endpoint security that is empowered not only to quarantine suspect software but to automatically patch and reconfigure security features.

But what if the endpoint security tool is a foe? What if a nation-state has spent months analyzing the operation of the tool, including client software, automated download sites and protocols, agent communication protocols, log repositories and console features? Potentially, someone with internal access and this knowledge could identify the access control mechanisms enabling secure operation and introduce configurations and executables that could turn the software from friend to foe.

## NETWORK DISCOVERY

Reconnaissance is a key element of any targeted attack. The easiest method to perform reconnaissance is with a professional asset discovery tool. Searching for the discovery tool in the TAG Taxonomy with its foe potential in mind, I started by scanning the detection categories. When I realized that of course “assets” would be a topic the Enterprise category, I still did not immediately land on it until I found it in the innocuous Enterprise subcategory of “Asset Inventory.” Asset Inventory refers to a relatively benign-sounding set of tools and techniques focused on ensuring that the scope of cybersecurity technology coverage is accurate.

As in any audit of assets, technology asset inventory is compiled via inclusion and exclusion tests on an authoritative listing referred to as the “inventory.” The listing sometimes contains all technology assets, including data and staff, and sometimes is limited to technology devices. Inclusion tests generally started with procurement and/or other types of onboarding records. That is, once an asset is onboard and before it is decommissioned, it is included in a listing of assets to be secured. Network discovery is the exclusion part of the test. If a device (or user or data) is automatically discovered in the enterprise technology environment that is not in the inventory (e.g., via a cybersecurity tool performing a network, credential or disk scan), the asset listing is assumed to be incorrect, and the discovered item is added to the listing. The next step is either to properly identify and document the asset, or to retire it.

Most enterprises treat such discovery tools as friends, helpful prompts to rope in shadow IT and unexpected contractors. These tools are often operated by junior analysts, and the data they collect does not typically meet business data classification as any level higher than “internal use only.” In many cases, the output of the network discovery tool is automatically “integrated” into an inventory repository, such as an enterprise configuration management database (CMDB). For example, a device discovery integration often consists of python or shell scripts that insert device records into the Asset Inventory that are marked as “discovered” rather than “procured,” thus creating to-do lists for technology operations to properly identify and catalog the device.

But what if the discovery tool is a foe? What if a nation-state has spent months analyzing the operation of the tool, as was done in Solorigate, including the tool’s scheduling, discovery protocols, data gathering and integration scripts? Potentially, someone with internal access and this knowledge could target the code in the integration scripts with injection techniques similar to those used against web applications calling SQL.

## PUBLIC KEY INFRASTRUCTURE

The weaknesses of PKI have been obvious since 2011, when the trusted certificate authority (CA) DigiNotar was discovered to have signed fake public keys for over 500 websites. The impact of this discovery cascaded from successful man-in-the-middle attacks on these sites to revocation of

**“Now that more nation-states are engaged in cyberwar, it is more and more probable that our trust in PKI infrastructure as a friend is overly broad.”**

DigiNotar as a CA by multiple browser publishers, causing unintentional denial-of-service attacks on legitimate sites, as browsers would no longer recognize their legitimacy. The issue was not resolved until DigiNotar was taken over by the Dutch government.

Yet PKI technology has not changed to reduce the risk that a fully trusted CA can knowingly operate for the dark side. In fact, with the increase in adoption of DomainKeys Identified Mail (DKIM), in which email headers are validated using a public cryptographic key in an organization's Domain Name System (DNS) records, reliance on PKI for site communication is even more prevalent. Ironically, secure DNS (DNSSEC) uses cryptographic digital signatures signed with a trusted public key certificate to prevent DNS spoofing and DNS cache poisoning. The history of those DNS attacks dates back to the DigiNotar time frame, and both attack types were attributed to nation-states even in 2011. Now that more nation-states are engaged in cyberwar, it is more and more probable that our trust in PKI infrastructure as a friend is overly broad, and PKI should be scrutinized for foe capabilities that negatively impact business.

## CONCLUSION

By design, cybersecurity tools tend to have overly broad access to data and operating system security configuration. Rather than being left off the list for application security testing, they should automatically be bounced to the top of the queue. Their treatment from a cybersecurity assessment perspective should receive the same rigor applied to critical business application cybersecurity risk review.





M Y  
T A K E

## A NEW ECOSYSTEM OF ALLIANCES

The conflict in Ukraine offers lessons on the dangers and opportunities in cyberwar.

DAVID HECHLER

Russia's invasion of Ukraine had the effect of reaffirming the value of weakened alliances that had sometimes seemed broken. The alacrity and strength of the response from Western countries seemed to surprise even the countries themselves. But Ukraine President Volodymyr Zelensky pressed his Western supporters for even more, which led to public discussions about how far nations could and should go to support Ukraine, which is not a member of NATO or the EU, without stumbling into World War III.

There were legal questions that Zelensky undoubtedly understood very well, since in addition to being a comedian he's also a lawyer, but under the circumstances he obviously felt compelled to play every card at his disposal. That included requesting that sympathetic countries impose a no-fly zone over Ukraine, which none was willing to do.

Beneath discussions about the kinetic war—about rules of engagement and potential war crimes—there were much quieter ones that involved the ongoing cyberwar. But the volume of those conversations did not render them inconsequential. Quite the contrary. They raised important issues. And these may grow if, as some observers believe, the cyberwar expands. As of early April, there were predictions that Russia would target countries that were punishing it with sanctions.

It's impossible to guess how long the war will last. But it's not too soon to draw some lessons from both the kinetic war and the cyberwar—and, for the latter, try to place those lessons in some semblance of context.

### CALLING FOR REINFORCEMENTS

One early development on the cyberfront of the Ukraine conflict was that proxies and partners on both sides sprang into action almost immediately. Shortly after Russia invaded, for example, Microsoft

**“Piecing together an ecosystem of cyber defenders based on a coalition of unvetted volunteers does not seem to be a model for future conflicts.”**





Corporation **detected “wiper” malware** that appeared to be aimed at computers in Ukraine’s government ministries and financial institutions. Within three hours the company was able to update its antivirus software to block the code, which can erase data on computer networks, and alerted Ukraine officials to the danger.

United States government personnel were also working to buttress Ukraine’s cyberdefense. “Hidden away on bases around Eastern Europe,” The New York Times **reported**, “forces from United States Cyber Command known as ‘cybermission teams’ are in place to interfere with Russia’s digital attacks and communications—but measuring their success rate is difficult, officials say.”

There was plenty of action on the offensive side as well. There was no immediate attribution on initial attacks, but it was easy to identify some of the hackers who took up the fight. The Ukrainian government called on its “IT army” of more than 200,000 followers on its Telegram channel to take down the websites of the Moscow Exchange and Sberbank, which they promptly did, The Wall Street Journal **reported**. The hacker collective known as Anonymous also got into the act by stealing and releasing information from the Russian Defense Ministry. Russia had its own professed vigilantes. The ransomware gang known as Conti quickly announced that it would attack Russia’s enemies in the war.

It was a marked contrast to the kinetic war in which sympathetic nations shipped arms to Ukraine and inflicted economic damage on Russia, but resisted any urge to participate directly. On the cyber side, it looked like anyone could join the battle. There seemed to be a free-wheeling, feel-good atmosphere of competing patriotism. But cybersecurity experts **warned of inherent dangers**.

First there’s the matter of attribution. It’s not an amateur’s game. Sophisticated attackers may disguise their identities, and those eager to retaliate may assume they already know the origin of an attack and the identities of the individuals responsible. If they’re wrong, they may badly damage the cause they think they’re supporting.

## THE RISKS OF FREELANCING

The kind of freelancing the Ukrainian government seemed to welcome invites additional misadventures. Attacks against Russia’s communications networks, for example, could disrupt intelligence gathering by Ukraine or its allies. Or uncoordinated attacks could hamper the Ukrainian government’s own offensive efforts.

Beyond that, there could be other unintended consequences. An effort to hack back could damage Russian citizens who bear no responsibility for the war, including those who may oppose it. And some attacks could harm people and organizations that have nothing to do with the conflict or the combatants. “If an affected organization is connected to hundreds of other organizations,” Andrew Rubin, CEO of cybersecurity firm Illumio, told The Wall Street Journal, “how do you make sure your attack doesn’t cause harm to all the connected systems?”

It may seem incongruous to bring up the legal norms of cyberwar at a time when Russia is being accused of war crimes in its bombing and alleged torture and execution of civilians, but the **Tallinn Manual 2.0** does note that under international law, nation-states are generally held to be responsible for the actions of their proxies. And this means that they are required to exercise due diligence in supervising and directing their actions. Having issued a call to action to thousands of hactivists, Ukraine is obviously in no position to fulfill that obligation.

Piecing together an ecosystem of cyber defenders based on a coalition of unvetted volunteers does not seem to be a model for future conflicts. It seems more like an act of desperation (however understandable that may have been). But perhaps a combination of the kinetic and cyber responses to Russia’s attack is worth considering for the future possibilities it may offer. And it might build on glimmers of progress that surfaced in 2021.

## NEW COALITIONS?

Last year featured dramatic international cyberattacks that spurred countries to work together to defend their security against gangs that operated from Eastern Europe, including Russia. Ukraine even figured into the mix. And a group of nations agreed they needed to work together to bring down the threat.

The biggest threat was ransomware. And the initial responses had been weak. The U.S. had drawn a red line years earlier in negotiations with China that said nation-states could use cyber for espionage, as nearly all countries do, but not for economic gain. The bad actors in ransomware attacks, however, were not nation-states. They were criminal gangs that were putatively independent of governments like Russia and China—but were protected by them because, without extradition treaties, the governments wouldn't extradite gang members to the countries where the victims were located. So ransomware attacks did not cross a red line, and there was no deterrence to keep gangs from operating with impunity.

But in May, after Colonial Pipeline was hit with a ransomware demand by the Russian gang DarkSide, President Biden was under great political pressure to do something. He was essentially forced to confront Putin and demand action. When he did, it led some of us to wonder [what had happened to the red lines](#).

It turned out they'd moved. Administration officials said Russia seemed open to discussing the issue, but the government didn't wait. Biden brought it up at the G7 summit last June, which led the group to issue a statement demanding that all countries crack down on ransomware gangs in their jurisdictions. In July, the FBI managed to claw back a portion of the ransom Colonial Pipeline had paid DarkSide.

**“Last year featured dramatic international cyberattacks that spurred countries to work together to defend their security against gangs that operated from Eastern Europe, including Russia. Ukraine even figured into the mix.”**



The government sought to broaden the potential coalition last October. It invited representatives from more than 30 countries to a [virtual meeting](#) in the White House on ransomware. One of the messages the participants heard: It was time to view ransomware attacks as a national security issue, rather than just another criminal matter. Coincidentally, they also heard a success story from Ukraine, where the FBI and international law enforcement had recently arrested two members of a ransomware gang and seized \$375,000 in cash.

Then in January, when many observers had probably given up on the idea that Russia would take action on Biden's demand—if they had ever even entertained such a notion—Russia [announced](#) it had arrested several members of the ransomware gang REvil. The timing was another reason for skepticism. The U.S. and Russia had just completed unsuccessful negotiations to try to avoid a war in Ukraine, and there was deep suspicion that the announcement was pure PR. But in March, after the war had begun, one gang member was extradited to the United States from Poland, where he'd been waiting in prison since October.

## TAKEAWAYS

These were small signs of progress, to be sure. But coupled with some of the lessons that can be drawn so far from the war in Ukraine, maybe they point to topics worth further discussion.

1. It's time to think of cyberattacks as national security issues. And not just those attacks launched by nation-states.
2. Countries should view damaging cyberattacks that are not for the sole purpose of espionage, and that emanate from nation-states that are either directly responsible for the attacks, or protect the perpetrators who are, as tantamount to acts of cyberwar. They should carefully document attribution and bring indictments that lay out the evidence against the alleged perpetrators. And they should work collectively with other countries, especially those that have also been victimized, to pressure the nation-states to extradite the accused to face charges. If there's no response, sanctions and other punitive measures should be considered.
3. Defensive actions such as those that Microsoft and the U.S. government took to aid Ukraine when it was under attack should be praised when the attack is unprovoked and a clear violation of a nation's sovereignty.
4. Defensive actions designed to aid a combatant in a cyberwar can also prove dangerous, even when widely viewed as justified. They can draw a country and its residents into conflicts they may not desire and for which they may not be prepared. And for companies, such actions may prove unpopular with shareholders. They would be wise to follow Microsoft's lead and publicly explain their rationale.
5. Offensive actions by freelancers during a cyberwar are dangerous. Even when they are requested by one of the combatants. We may never know whether the actions by the hackers invited to join in by the Ukrainian government did more good than harm for its side. It appears the government did seek to direct the efforts of some of those participants. But once the invitation is public, there's no telling who will take up the cause—and with what results.
6. In a world riven by misinformation and disinformation, nothing is simple. Even without the fog of war. Attribution of attacks should not be based on assumptions. It should be the province of trained professionals.
7. Coalitions of nations that take action in order to combat the dangers of cyberspace, and are willing to do so even when they incur economic or other painful costs to try to resolve or reduce those dangers, can accomplish important things. The hardest task may be to convince them to start acting, and to continue the effort, before the conflict spins out of control. This is particularly challenging because so much about cybersecurity is not visible to the general public.
8. It is not possible to eliminate all crime. But criminals cannot be allowed to operate without deterrence. A class of criminals that can steal with impunity from people around the world just because they're sitting in a certain location should not be tolerated.



# INTERVIEWS



AN INTERVIEW WITH CANDID WÜEST,  
V.P. OF CYBER PROTECTION RESEARCH, ACRONIS

## UNIFYING CYBER PROTECTIONS ACROSS THE ENTERPRISE

Every company has come to understand the importance of coordinating IT and security initiatives to reduce cyber risk. One major example involves the use of trusted backup and restoration to address both day-to-day IT infrastructure as well as the growing risk of ransomware and other destructive attacks.

Acronis offers comprehensive protection for a wide range of IT and cyber-related risks to the enterprise. We wanted to gain insights into the company's priorities and how it has addressed a constantly changing cyber threat landscape.

***TAG Cyber: What are some of your key priorities in cybersecurity for the coming year?***


**ACRONIS:** It's been shown that many organizations struggle to keep up with cyber protection due to the complexity and lack of resources. Our priorities are therefore to further optimize the consolidation and automation of cyber protection tasks for organizations. These include cross-correlation through artificial intelligence, expanding integration and simplification of protection and mitigation. For example, we're launching our new DLP and EDR packages this year to provide further capabilities. The important focus here is to make them as easy and automated to use as possible, so companies don't have to build a full SOC team just to interpret the product alerts.

***TAG Cyber: How have ransomware attacks evolved and how does Acronis help reduce this risk?***

**ACRONIS:** Ransomware groups are increasingly taking advantage of living-off-the-land techniques and existing infrastructure tools. Especially with service providers and global organizations, tools such as those for software deployment have huge access to the entire infrastructure. Once the attackers have elevated their privileges, they uninstall security and monitoring tools, delete backups from the console, and use backup or cloud tools to exfiltrate data. Adding hidden backdoors to backups is another all-time favorite of attackers. As for encryption, we see many groups trying to inject into trusted processes and distribute the work over multiple processes in hopes of bypassing traditional detection heuristics.

A recently leaked internal document from the Conti ransomware group revealed that it had made over \$2.7 billion from extortion payments. Most other groups don't make as much, but everyone wants to, so there's no end in sight for ransomware attacks. Acronis Cyber

Reliable system backups that can be efficiently restored, or even a complete disaster recovery plan to minimize business disruption, can make all the difference if an organization wants to survive a cyberattack.



Protect uses a multi-layered holistic approach to defend against this wave of ransomware attacks. Detecting never-before-seen ransomware based on its behavior and automatically restoring all compromised files from a protected cache is a crucial part of it. Additional features, such as immutable storage or self-protection of the security component, help make it more difficult for the attackers. Of course, basic functionalities such as network segmentation and strong authentication should be implemented as well.

***TAG Cyber: How do you ensure that backups cannot get re-infected during an attack?***

**ACRONIS:** We provide a unique deep integration of backup and cybersecurity in one agent. This allows the service not only to scan each file before adding it to the backup, but also to run periodic scans of the backup in the cloud. By offloading these scans, you can be more aggressive and detect rootkits and other malware in their dormant states. Before restoring a backup, it can be scanned and patched to minimize the risk of immediate re-infection.

***TAG Cyber: Tell us about how cyber insurance and related risk measures should be integrated into an enterprise protection program.***

**ACRONIS:** As with IT security in general, organizations must conduct regular risk assessments and identify the greatest risks to their business. Cybersecurity and data protection solutions can help minimize these risks, but they won't be fully eliminated. Organizations can then decide to cover some of the risk through cyber insurances, depending on their own risk appetite. Insurance policies help cover the financial losses that result from cyber incidents, but they won't prevent the impact from happening. It's important to read the fine print and check which cases will result in payouts, as some insurers have excluded specific cyberattacks.

***TAG Cyber: Do you believe that trusted backup protection will play a key role in future global cyberwar activity?***

**ACRONIS:** Cybersecurity alone is unfortunately no longer good enough to protect your organization well. There will always be some attack slipping through or taking time until the analyst verified the EDR/XDR alerts. Reliable system backups that can be efficiently restored, or even a complete disaster recovery plan to minimize business disruption, can make all the difference if an organization wants to survive a cyberattack. A trusted backup that has been scanned for backdoors and stored in multiple safe locations that can't be deleted by the attackers is an important lifeline. Being able to minimize interruption by spinning up such backups up as virtual machines can further reduce the cost of cyberattacks. As the complexity of sophisticated attacks continues to increase, defenders must increase visibility and holistic responses to their infrastructure to keep pace.



AN INTERVIEW WITH JUHA HAAGA,  
HEAD OF MARKET RESEARCH, ARCTIC SECURITY

## AN EARLY WARNING SERVICE FOR CYBERSECURITY

Early warning systems have served humankind as an important defense against catastrophes and hazards, both natural and man-made. Now we need them to protect us in cybersecurity. The challenge is that finding early evidence of breaches and vulnerable services requires expertise and care.

Arctic Security provides a cybersecurity early warning service for its customers. We want this capability to be deployed to protect enterprises and to reduce cyber risk.

***TAG Cyber: How does your early warning service work?***

**ARCTIC:** We collect high quality data from many sources. Then the data is harmonized, categorized and matched to the owner of the assets. IT people are often overwhelmed with things to do, so many security issues go unaddressed. We take the essential information about the issue and provide it to the customer.


***TAG Cyber: How does your service integrate with enterprise threat intelligence platforms?***

**ARCTIC:** Our customers often integrate with ticketing systems so issues can be remediated. The data from Arctic is also used with incident response and management systems and SIEMs. We provide an outside-in view and help catch things that may have missed detection.

***TAG Cyber: How do you help customers decide what is actionable and what is not?***

**ARCTIC:** Determining whether the information is actionable has been an industry problem for a long time. Consumers of the threat intel services have been overwhelmed with information. We solve that problem by turning it around. Arctic EWS only takes in actionable information that we provide to our customers. Our early warning service ensures that the customer gets the credible pieces of information without having to filter it themselves from the data. When we add a new type or category of a cybersecurity problem to report about, we walk the extra mile to ensure that it's good. The volume of data we provide to our customers is much lower, but when we

Our early warning service ensures that the customer gets the credible pieces of information without having to filter it themselves from the data.



send the information, they know to stop what they're doing and address the issue.

In addition, Arctic Security incorporates features of external attack surface management into our service, so that Arctic EWS subscribers can have better awareness of their whole asset footprint. Many business-related services are outsourced to vendors and there is typically very little visibility on those. With Arctic EWS, we extend continuous monitoring and alerting to those assets. We do automated classification of assets to let them know when there are issues such as exposed databases that are worth taking up with their vendors.

***TAG Cyber: Tell us more about the types of threats you include in your warning service.***

**ARCTIC:** Early warning threats can be roughly divided into four categories. The most common one is information about vulnerable internet-facing services, which is used to proactively close weaknesses in corporate networks. This directly reduces the opportunities that cyber criminals have. We track both newly released vulnerabilities, and the long tail of vulnerabilities that linger for years. Unpatched systems may get exposed in network reconfigurations and other mistakes.

The second most common category is potentially compromised systems. This is information about malicious activity already originating from the early warning service customer's network. Observation in this category means that there is an ongoing cybersecurity problem, and it's urgent to address it right away. Since typical dwell time is measured in days, it's still an early warning from the perspective of preventing lateral movement and prospective ransomware attacks.

The third category is leaked credentials. We inform our customers when their credentials are discovered in various data leaks, so that they can ensure that those credentials and passwords are not shared and in use by their employees. This prevents exploitation opportunities.

A fourth category is open services. Companies open services to the internet, and they may not be vulnerable at that moment, or it may not be possible to identify a vulnerability from the outside. However, many of these services have patchy security histories that include known exploitation in the past, and organizations should be aware of their attack surfaces, in case a new exploit becomes available. Often these services do not need to be open to the internet in the first place, and a lot of damage can be avoided by removing them before something bad happens.



**TAG Cyber: Do you think an early warning service can play a significant role in a future global cyberwar?**

**ARCTIC:** Cybersecurity enterprises and civil infrastructure may be targeted or suffer collateral damage both in conflicts and during peace. From the perspective of the defender, the first priority is not to worry if the attacker is a criminal, a cyber mercenary or a state actor. Instead, it should be proactively make attacks harder and detect failed defenses quickly. A good early warning service will help harden the defenses and act as a deterrent through improved detection and response. It's hard to say how significant it will be in future global cyberwar, but it's easy to say that it's a no-brainer in everyday enterprise life.



*“I been thinkin’ on whether to grab s’more Crowdstrike stock or just fix the damn porch.”*



AN INTERVIEW WITH GUY FLECHTER,  
CEO, CIDER SECURITY

# ENSURING SECURITY FOCUS ACROSS DEVOPS

Every software developer knows the importance of cybersecurity during DevOps and CI/CD pipelines. Without good tooling, security automation and control, the likelihood that software will be produced with vulnerabilities is high.

Cider Security is working this problem with emphasis on keeping pace with modern DevOps teams. They explained their vision for supporting engineering and operations teams during all phases of the application software lifecycle.

***TAG Cyber: Why have developers traditionally not focused on security during the production of software?***

**CIDER:** This gap originates from a combination of three factors. Security teams have a difficult time obtaining a deep understanding of the technologies, frameworks and processes that exist in the engineering ecosystem. Another challenge they face is in understanding and prioritizing risks associated with the organization's engineering ecosystem, and deriving the appropriate measure and control required to optimize security across the full engineering journey—from code to deployment. Lastly, it takes time and effort for engineers—mainly DevOps—to implement security scanners and engines within engineering processes and systems, and to understand and mitigate security-related findings generated by these scanners.

These factors ultimately lead to a situation that is far from optimal. Security teams are struggling to promote the security agenda within the engineering ecosystem, often placing focus and emphasis on initiatives that don't yield effective outcomes; whereas engineering groups are often left with the inevitable sentiment that security controls are ineffective and not tailored to their needs, slowing down the pace of engineering without providing enough value.

***TAG Cyber: How does automation help reduce risk during DevOps?***

**CIDER:** Automation is a critical element in any security work. The need to move fast without the barriers of having enough employees on the security team is critical for any company.

Cider's solution establishes connectivity to the different systems across the engineering ecosystem and leverages the connectivity to build the ecosystem's assets inventory.

Because the DevOps environment is moving really quickly, there is a need for automation that can help move the information with equal speed to the engineering team without the need for manual work.

**TAG Cyber:** *How do you build proper tooling to support DevOps?*

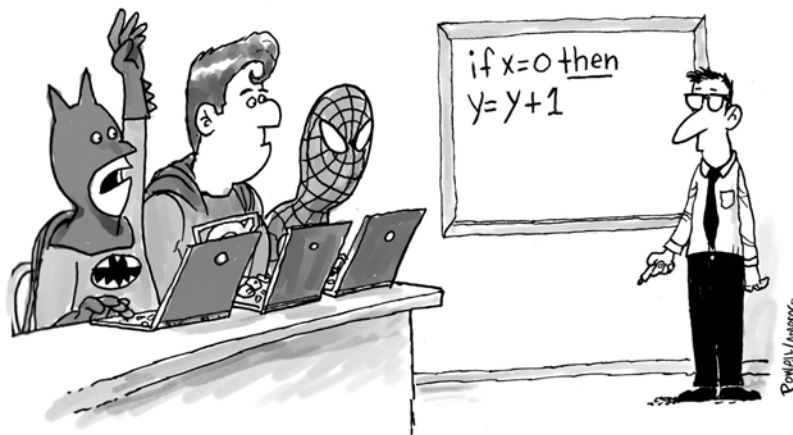
**CIDER:** To build a proper tooling you need to have a good understanding of the DevOps ecosystem, which is a very complex one. Only after you are able to get the full understanding can you start building the proper tooling.

**TAG Cyber:** *Tell us more about how your platform solution works.*

**CIDER:** Cider's solution establishes connectivity to the different systems across the engineering ecosystem and leverages the connectivity to build the ecosystem's assets inventory. This allows security teams to understand the technical characteristics of the engineering environments' systems and processes, which they use to understand the risks and, ultimately, to weave in various engines and solutions tailored to the organization's technical stack—with zero reliance on DevOps.

**TAG Cyber:** *Do you believe security tooling during DevOps will play a role in future global cyberwar?*

**CIDER:** I think that any security tool in any place is playing a role in future global cyberwar. If we look specifically at DevOps, we can already see a lot of nation attacks on the DevOps area—for example, Solarwinds.



*“So, workload containers are basically little Batcaves for apps?”*



## AN INTERVIEW WITH KAILASH AMBWANI, CEO, CONSTELLA INTELLIGENCE

# SAFEGUARD YOUR PEOPLE, DATA, AND BRAND THROUGH DIGITAL RISK PROTECTION SERVICES

The business world's growing dependence on digital services continues to increase the volume and range of external digital threats aimed directly at executives, employees, brands, operations, and infrastructure. To respond, organizations must employ proactive measures to monitor malicious activity, collect intelligence and provide proactive, actionable guidance.


Constella Intelligence meets this challenge via Dome, an advanced digital risk protection platform that not only defends people but protects data and ensures the integrity of corporate brands. We were eager to learn more about these services and how they can be employed across an enterprise.

### ***TAG Cyber: Why do employees need digital risk protection?***

**CONSTELLA:** That's an excellent question, because many organizations assume that only senior executives are targets for external threats. In fact, every employee with access to valuable internal assets needs digital risk protection. While the volume of digital transformation initiatives multiplied rapidly in the years prior to 2020, that process accelerated at a staggering rate during the COVID pandemic—compressing seven years of development into just a few months, according to a McKinsey study. As a result, digital transformation now means that most knowledge workers have access to critical systems and data, even as they typically lack corporate-grade security practices and protections.

Threat actors know these trends, and the opportunity they present. That's why compromised credentials and exposed personal information now represent the most common vector for data breaches, and they enable account takeover (ATO), ransomware and phishing attacks. To be clear, executives and VIPs remain primary targets, and the visibility and status of these individuals mean a different level of threat. Executives face online impersonation, hacktivism, reputation attacks and doxxing, all of which affect brand and market value and, in extreme cases, personal safety for them and their families. Recognizing that executives and employees face different types of threats, we designed our Dome platform to provide two tiers

## Many attack techniques aimed at executives also impact brand reputation, including impersonation profiles, fake social media content and hijacked accounts.



of protection: Employee Protection for common threats aimed at employees, and Executive Protection for enhanced defenses against a broader range of attacks. We also ensured that the Dome platform had the massive scalability and automated, continuous monitoring to protect everyone with access to sensitive data and systems, regardless of the size of the organization.

### ***TAG Cyber: How do these external threats extend to corporate brands?***

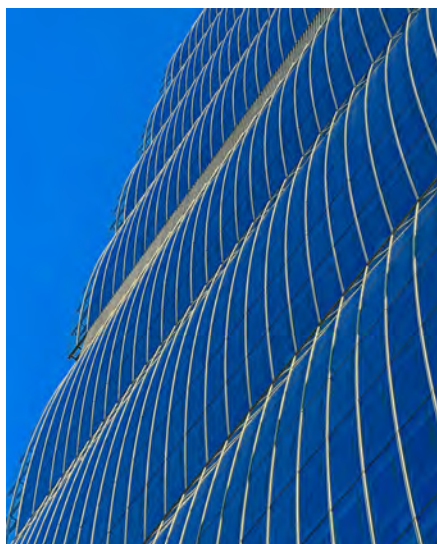
**CONSTELLA:** Many attack techniques aimed at executives also impact brand reputation, including impersonation profiles, fake social media content and hijacked accounts. The difference is they target corporate, rather than individual, accounts and profiles. In addition, brands also face the threat of stolen intellectual property, counterfeit products and viral campaigns that can cause extended damage to the brand. Clearly, organizations need the ability to recognize and respond to attacks against their brand from impersonation sites, defacement of online properties or phishing campaigns targeting customers. However, they also need to be able to know if malicious online activity originates in online communities where threat actors congregate, and understand the nature of the conversations in those closed forums or messaging platforms.

These capabilities will become even more essential as digital geopolitical threats grow in frequency and severity. The good news is that the same automated, continuous monitoring and analytics within our Dome platform that protect executives and employees also can monitor brand-related malicious activities, because we monitor thousands of sources across the surface, deep, and dark web as well as social media. Organizations gain the ability to identify these external risks targeting their brands sooner and respond proactively to limit damage.

### ***TAG Cyber: Tell us more about how to address geopolitical threats.***

**CONSTELLA:** Geopolitical threats illustrate how multiple threat vectors intersect, such as a coordinated group of threat actors targeting an organization to discredit the executive team, steal data, damage the brand and launch a viral disinformation campaign. In short, all these techniques are now central components of international conflict.

Businesses need immediate insight into rapidly evolving political, economic and social situations within or across geographic regions to be able to minimize damage from geopolitical threats. Monitoring across a massive volume of data from diverse sources provides immediate awareness of everything



from compromised credentials and exposed personal data on the dark web to fabricated social media content to discussions of floorplans of facilities. With this visibility, organizations can anticipate and defeat digital risks.

The scope of geopolitical threats has expanded rapidly over the last decade, with the volume of online threats surrounding the Ukraine invasion illustrating its scale and impact. That's why our Geopolitical Protection module in Dome provides automatic, scalable and continuous monitoring for regional and global geopolitical threats, including hostile narratives aimed at brands or individuals. This intelligence enables the ability to identify and track key threat actors, anticipate and inform decision-making and adjust response strategy to counter dangerous situations driven by political activism, social activism or critical events.

***TAG Cyber: How do you deal with social media?***

**CONSTELLA:** Social media is often overlooked as a significant threat vector to organizations, yet it requires automated, continuous digital risk protection across the full breadth of the internet. Social media platforms, both regional and global, play a significant role in executive impersonation, brand impersonation, disinformation and even employee safety. The reason social media is so important to monitor is because it provides a fertile ground for digital activism and influencer-driven pressure campaigns. It enables the creation of private spaces for organizing coordinated online or physical activities. To counter these threats, only continuous monitoring of a range of social media platforms enables organizations to recognize misinformation campaigns, reputation attacks or rallies at facilities, and then take pre-emptive action to minimize operational disruptions. However, these activities require more than the ability to track what's happening. They also necessitate the ability to monitor context and intent. In this scenario, multilingual capability and advanced AI become the keys to separating benign conversations from situations that demand corporate protection and response. Few businesses can track and analyze the global social media landscape on their own, especially across less visible platforms. However, understanding these threats is a next-level type of protection that should be on every corporation's must-have list, and we now feature it as part of our Dome platform.



## AN INTERVIEW WITH WITH KISHOR VASWANI, CHIEF STRATEGY OFFICER, CONTROLCASE

# SUPPORTING COMPLIANCE AS A SERVICE

IT Security and compliance are greatly complicated by the myriad different frameworks and certifications that are required for the typical enterprise. These include PCI-DSS, HIPAA, ISO, and many more. For most organizations, the only reasonable solution has been to automate the process, and IT governance, compliance, and risk (GRC) tools have thus emerged as one of the most important aspects of modern enterprise security.

We recently spent time conversing with Kishor Vaswani from Fairfax-based ControlCase to develop insights into how they are streamlining this automation with compliance solutions that are delivered in an as-a-service manner. The results appear to be successful, and we were keen to understand whether this approach might help more enterprise teams deal with their compliance burden. Here is a brief digest of our conversation:

***TAG Cyber: Tell us first about the company. When were you founded and what's been your value proposition for enterprise customers?***

**CONTROLCASE:** ControlCase was Founded in 2004. We excel at two things:

1. We help companies achieve their IT security certifications with ease and without breaking the bank. We certify to regulations including PCI DSS, SOC, ISO 27001, HIPAA, GDPR, etc.
2. We provide a technology-driven continuous compliance solution that provides peace of mind that environments are secure and risk is reduced.

***TAG Cyber: What has been your experience in assisting customers with their compliance? Has it been the process? Attestation? Understanding the requirements? Perhaps all of the above?***

**CONTROLCASE:** Great question! What really sets us apart is that we are not a checkbox auditor; we adopt a partnership approach in all our engagements. So, because of that, we start at the beginning—really understanding our customer's environment and exactly what is driving them in their compliance process. We become an extension of their IT security compliance team to understand their motivations for, business processes used, and any gaps between current state and achieving compliance. Then we support them through remediation before moving to a final audit. To answer your question directly, it's really all the above; we have a tried and tested methodology that takes away audit fatigue for our customers and gets us to our goal in harmony.

To be honest, many of our clients battle with the issue of which regulation they need to be compliant with.



***TAG Cyber: Do you see the possibility of some compliance framework consolidation in the coming years? It sure seems like there might be too many different security compliance requirements standards.***

**CONTROLCASE:** Yes absolutely; our research has found that most of these IT security regulations can be easily mapped to each other. To be honest, many of our clients battle with the issue of which regulation they need to be compliant with—because you're right, there are so many.

As a result, we support clients who require compliance with multiple regulations so the mapping we have done eliminates repetition and saves both time and money. We certainly see consolidated frameworks coming in the future.

***TAG Cyber: How are customers responding to your One Audit approach? Do they have to modify their internal compliance programs to use your service, or has the integration been simpler?***

**CONTROLCASE:** Another great question! Companies that care about security have been very responsive to our One Audit solution. In a nutshell, it allows us to collect evidence once and certify companies to multiple regulations. Because we partner with our clients and understand the business requirements that are driving the need for multiple certifications, we have really focused on using smart technology to enable automation. This has created a seamless solution that integrates with clients' environments so that we can collect evidence more efficiently, manage security and continuous compliance, as well as keep costs and stress to a minimum.

***TAG Cyber: What do you see on the horizon for compliance programs? Do you see integration of security and privacy certifications, for example?***

**CONTROLCASE:** I believe compliance programs are going to become more stringent—the easier it is and the more we share data, the more stringent these regulations will become. And I believe it is a necessary transformation that has already started to happen. Most regulations cover aspects of both security and privacy—it's just that there is usually a choice on the privacy aspect. In answer to your question, I truly believe we will eventually come to a place where compliance programs find the perfect harmony between security and privacy





AN INTERVIEW WITH BRIAN DYE,  
CEO, CORELIGHT

## LEVERAGING THE POWER OF OPEN SOURCE-BASED NETWORK DETECTION AND RESPONSE

Powerful open source tools, such as Zeek® for network security monitoring, have existed for many years to help security professionals gain visibility into potential threats and malicious activity on their networks. However, deploying and maintaining these platforms in large enterprises is often challenging.

This is where Corelight comes in. Co-founded by Dr. Vern Paxson, the creator of Zeek, Corelight extends Zeek's powerful network monitoring capabilities and simplifies deployment. The result is a Network Detection and Response (NDR) platform that transforms network and cloud activity into evidence for complete visibility, powerful analytics, faster investigations and advanced threat hunting capabilities.

**TAG Cyber:** *What are the pros and cons of using open source tools such as Zeek for security?*

**CORELIGHT:** Zeek's popularity is from the quality of the evidence it provides: rich, interconnected insight into activity on the network. That insight has evolved through two decades of work done by elite defenders around the world, so those using it today benefit from the knowledge of over 10,000 global deployments and over 100 community-contributed projects. Beyond that, the organizations can customize the evidence and build their own analytics. Finally, because of the large community, there is a training ecosystem that makes it easier to enable security analysts.

However, open source platforms are notoriously difficult to deploy and maintain. Most open source Zeek is not security-hardened, doesn't have protections for overloading, and lacks the automation hooks or central management that the Corelight versions have. Deploying the platform can easily take months for a commercial enterprise environment. Operating and maintaining an open source solution on your network typically requires someone very well-versed in the technology to maintain it. If that person, or team, leaves the organization, so does the knowledge required to run the platform. Finally, actually operationalizing the solution—ensuring that the technology is part of processes and workflows and used in the day-to-day operations of a SOC—often doesn't happen, and the solution becomes either shelf-ware or a limited use product. This was the guiding principle behind Corelight: Create an enterprise-ready, easy-to-deploy version of Zeek while ensuring that the open source project and its community

This was the guiding principle behind Corelight: Create an enterprise-ready, easy-to-deploy version of Zeek while ensuring that the open source project and its community would continue to thrive.



would continue to thrive. Our customers benefit from that ease of deployment and keep the customization capability while still evolving with the community of elite defenders.

***TAG Cyber: How does the Corelight platform work?***

**CORELIGHT:** Essentially, the platform receives a copy of the network traffic from a packet broker or cloud TAP that the customer already uses. We then analyze the traffic, generating both alerts and forensic and security-oriented metadata logs about that traffic. The resulting alerts, data files and logs are then fed into the customer's SIEM. Together, these give incident responders and threat hunters the data—or, as we call it, the evidence—they need, in a standardized format that's easily searched and integrated with existing security tools.

***TAG Cyber: How do you provide support for network security teams using Corelight who have deployed Zeek already?***

**CORELIGHT:** While we don't provide support for open source Zeek directly, we do help customers transition to Corelight by providing a world-class customer support experience. We invested in customer support very early on; you could consider that part of our founding thesis. If we wanted to make open source easier to use, customer support would be key. We can both load any existing scripts they have on top of the prepackaged collection of detection or log augmentation scripts we include, so they don't need to leave behind their hard-won customizations. While no upgrade is completely automatic, we strive to make it as painless as possible and offer professional services to buff out any rough edges.

***TAG Cyber: Tell us more about how your solution drives a full NDR capability for enterprise.***

**CORELIGHT:** Full network detection and response capability is really about driving an evidence-based strategy. There is plenty of technology that drives "alerts," and we do that too. Corelight's deep packet inspection allows us to both generate alerts (signature, behavioral, ML, etc.) and provide full telemetry surrounding those alerts, for both network and cloud activity. Customers leverage that telemetry or evidence to triage those alerts, proactively hunt for threats and leverage machine learning and other tools to stay ahead of attacks. We saw this with both the Solarwinds and Log4j attacks. The malware and vulnerabilities were missed by EDR, IPS/IDS and other solutions. But even the most sophisticated hackers leave footprints on the network, and our evidence helped customers find those, and we were able to create and provide detections through both the Zeek and Suricata community within 48 hours. This particular example underscores the value of Corelight—an NDR platform built on top of open source provides a very robust solution for enterprise customers.

***TAG Cyber: Do you have any predictions about whether tools such as yours can play a role in future global cyberwars?***

**CORELIGHT:** The simple reality is that there is no real way of knowing what type of attack a nation-state might wage in a cyberwar. Even with the current conflict between Russia and Ukraine, we still don't really know exactly what Russia has planned or has done. We have not seen the major attacks to critical infrastructure that we were worried about, but that doesn't mean it hasn't happened yet. As we saw with Sunburst and Log4shell, the only real protection against those kinds of advanced attacks is to have the evidence you need to look back in time. That evidence both enables threat hunting and helps defenders investigate threats discovered later. The network is essential as attackers can't really avoid it. They can evade endpoints, obfuscate identity and hide somewhat with encryption, but there is always a footprint somewhere on the network.

We are closely monitoring the global landscape, taking guidance from U.S. government entities such as Cybersecurity and Infrastructure Security Agency (CISA). CISA's recent **"Shields Up" memo** outlines the tactics, techniques and procedures (TTPs) that defenders of critical infrastructure should look for. We took that information and provided **guidance** to our customers on finding TTPs, such as VPN misuse, spear phishing, and exploitation of known vulnerabilities, using network data. In addition, we help customers look for IP addresses of known nation-state entities and can help look for signs of "unusual behavior" that should be investigated. For example, our platform is the only one that we are aware of that can flag Cyrillic keyboard usage on your network.



*"These autonomous mowers worry me."*



AN INTERVIEW WITH FRED KNEIP,  
CEO, CYBERGRX

## MANAGING THIRD-PARTY CYBER RISK

---

The challenge of addressing cyber risks in business suppliers, partners and even customers has gradually risen to the top of the list of challenges for most CISO-led teams. Simple questionnaires help but are generally insufficient to drive the type of risk management needed in most environments.

CyberGRX offers a creative approach to this problem via a third-party exchange solution. We were interested to learn more about how the platform is used in practice.


***TAG Cyber: What is the greatest security challenge companies have in dealing with third-party companies?***

**CYBERGRX:** Enterprises across all industry sectors are relying more heavily on third-party vendors to conduct business operations and successfully achieve digital transformation. It's no surprise that third-party breaches are becoming increasingly more common as connected ecosystems are expanding. There is a significant problem with ineffective tools available in the market because they lack the ability to properly mitigate the risk posed by vendors and suppliers. The approach to effectively mitigate third-party cyber risk is broken. Organizations invest a great deal of money and resources into risk management strategies, yet still experience major gaps in their security postures. With a high focus on assessments and workflow processes, both enterprises and third parties are overwhelmed, mired in a volume of requests and data that is not actionable. Their resource contribution is high, yet confidence is low that they are truly getting what they need to determine where their actual vulnerabilities lie.

***TAG Cyber: How does the CyberGRX solution work?***

**CYBERGRX:** Traditional approaches to third-party risk management are centered around assessment collection, which is why these practices require so many resources. However, our platform is different. The focus is not on assessment collection, but rich datasets that provide immediate visibility into third-party risk. This data, compiled through the Exchange platform, is regularly updated to always show

One of the biggest misconceptions surrounding third-party risk is that collecting security assessments from your third parties equals reduced risk. This leads to enterprises sending out lengthy, redundant questionnaires to every third party in their ecosystem.



a third party's most current security posture. Our platform is scalable and accommodates a company's entire—and rapidly growing—third-party ecosystem. In summary, the Exchange replaces all the redundancies and outdated Excel spreadsheets with a standardized, cloud-based platform that enables users to access and share cyber risk data and actionable insights.

Our platform is driven by sophisticated data analytics, machine learning and automation, real-world attack scenarios, and real-time threat intelligence, providing customers with complete and ongoing analysis of their vendor portfolio. Organizations have the necessary tools to collaborate with each other, in a one-to-many environment, where they can share data and learn from each other's experiences.

***TAG Cyber: Do large and small companies use your exchange differently?***

**CYBERGRX:** Our platform works for any size organization. It operates on a Third Parties Under Management model, which means organizations can monitor and manage any number of cyber-relevant third parties. Cyber risk profiles are created for each third party individually, while portfolio-wide insights focused on business exposure, inherent and residual risk levels can be seen at both the individual and portfolio-side levels.

***TAG Cyber: Tell us more about trends in cyber risk management for third parties. Is the problem getting worse?***

**CYBERGRX:** One of the biggest misconceptions surrounding third-party risk is that collecting security assessments from your third parties equals reduced risk. This leads to enterprises sending out lengthy, redundant questionnaires to every third party in their ecosystem, and this antiquated approach to risk assessments is extremely burdensome to third parties on the receiving end. Traditional risk assessments quickly become a third parties' nightmare because they consume a ton of time and resources to complete. What's more, until they are completed oftentimes a sales team cannot make a sale—because the customer isn't satisfied that they have the cybersecurity information they need. Not only were risk assessments eating up tons of time and resources, they were also stalling the sales cycle.

However, the needle has started to move in the right direction. The threat landscape has drastically expanded through digital transformation initiatives, and organizations are now relying on more third parties than ever before. And they have finally realized that while waiting for an assessment to be returned, they are still vulnerable to an attack. As a result, many have begun to modernize their third-party cyber risk management strategies, easing the burden placed on vendors, but there is still a long way

to go. Organizations may now be getting questionnaires more quickly, but they're not necessarily the most accurate, creating a new problem. We need to see a shift towards gathering insights from the completed assessment data to receive greater visibility into the overall threat landscape, and then applying machine learning, threat intelligence and other tools to these datasets. Data is our most valuable asset, and we need to utilize it to identify gaps in the security posture of third parties before their companies, and even your own, face attacks.

***TAG Cyber: Do you have any predictions about whether third-party cyber risk management can play a role in future global cyberwars?***

**CYBERGRX:** Oftentimes, nations will initiate cyberwar even before troops hit the ground. And, even if your nation is not involved in the conflict, they are not immune from a cyberattack stemming from cyberwar. Our digital ecosystems are interconnected with companies all across the globe. Take the war between Russia and Ukraine. Even if you are not directly doing business with a company in Ukraine, one of your third parties might be, and an attacker can still get to you. It's now easier than ever for an attack on an organization in another nation to cross borders and seas, and even industries.

Cyberattacks have gone beyond data theft and encryption and now have more damaging consequences. During cyberwar, bad actors tend to target critical infrastructure first. And they'll do so through the path of least resistance, which is typically through third parties. When critical infrastructure is attacked, cybercriminals can shut down operational units, which results in no power, water, or other necessary resources. Third-party cyber risk management plays a pivotal role in cyberwar. It's no longer one nation under attack. It's all of us, and we have to defend ourselves differently to protect against an attack in these situations.



*“Our Security Awareness Message for April is just a simple ‘No’.”*



## AN INTERVIEW WITH COREY WHITE, CO-FOUNDER & CEO, CYVATAR

# MANAGING SECURITY FOR SMBs

---

The traditional view was that only large companies and agencies were targets of cyber threats. But this has since been replaced with the more accurate view that all organizations are targets. It's therefore sensible that managed security solutions have begun to emerge that meet the needs of this important small- and medium-sized business (SMB) segment.

Cyvatar offers fully managed security solutions with a complementary platform that includes many desirable features for SMBs. We were interested to gain some insight into how the solution would work in practice.

### ***TAG Cyber: What is the major cyber risk challenge for SMBs?***


**CYVATAR:** SMBs are a huge target because the cybersecurity industry doesn't care about them. The industry can't make money off smaller companies, so they tend to tailor their efforts toward larger companies. This leaves the SMBs to either figure it out themselves, or trust their local IT partner or managed service provider (MSP). SMBs are hit with large enterprise attacks, but don't have those large enterprise budgets or expertise.

### ***TAG Cyber: How does the Cyvatar solution work?***

**CYVATAR:** We're making cybersecurity "effortless and accessible" for our members. Most startups and SMBs do not have in-house security expertise, and they shouldn't. It's not cost effective to find and retain someone, and hope they have the expertise you need. And then, evaluating existing security products can take months. Finally, once inventory is acquired, you have to install, configure and maintain all products in-house. This is an inefficient process, even for larger companies. Cyvatar becomes an extension of your organization. We run your cybersecurity program, offering solutions—not just products, services and more alerts.

We identify your organization's security gaps, or we build a strategy from the ground-up, all within our proprietary platform before we sell you anything. We do not believe in selling solutions the member doesn't need. Our assessment gives us the insights we need to map out a security strategy for your organization based on your business goals and drivers. Do you need to become SOC 2 compliant? Do you plan to

**Most startups and SMBs do not have in-house security expertise, and they shouldn't. It's not cost effective to find and retain someone, and hope they have the expertise you need.**



hire aggressively? From there, Cyvatar and the member agree on a solution roadmap. We then execute on our proprietary ICARM Methodology (installation, configuration, assessment, remediation and maintenance) and you watch it all happen within the platform. From GRC, to implementing security policies, your issues and remediation, Cyvatar does it all.

***TAG Cyber: How do you deal with SMBs likely having little or no security staff to work with?***

**CYVATAR:** It's our bread and butter. Cyvatar was founded on making cybersecurity accessible, achievable, and cost-effective for SMBs. We become that security staff or augment existing staff. It's simple. We hire the experts in our solution portfolio that have done it all, dozens of times. It makes no sense to hire internal staff that don't have the experience or expertise when you can get the people, process and tech from Cyvatar, bundled into a single monthly cost that's more cost-effective than a single full-time employee.

***TAG Cyber: Tell us more about the services you include in your SMB offering.***

**CYVATAR:** We have mapped all the compliance standards to understand what the basics are. Our solutions include: ITAM—IT asset management. This's important because you can't secure what you don't know you have. For example, how can you patch a system facing the internet if you don't know it exists and what software is running on it?

TVM—Threat and vulnerability management is a staple solution that every company needs. It includes continuous vulnerability scans, because approximately 50 new vulnerabilities come out per day. So, the reality is you can't scan weekly or monthly because you will miss something for sure. The scanning is just the identification you have to fix it in a timely manner. So, we partner with our members to create a patch management program. And we partner with the member again to fix the non-patch related vulnerabilities. We get our members to maintenance in 90 days or less.

CSM— Cloud SaaS management is a critical solution because it helps secure newer companies that do not have a firewall, or any infrastructure. It accesses cloud-based services for log review and alerting of SaaS solutions like Microsoft 365, AWS, Slack and G-Suite, to name a few.

SEM—Secure endpoint management is a core solution that all companies need. We use next gen AV that has the capability to block malware from executing. Most companies fail here because they use legacy AV and are not able to identify next gen malware. The second failure is that either they don't have the



capability to block the malware; or, if they do, it's not configured. That's like having an amazing door lock on your house and never using it.

MSAT—Managed security awareness training is absolutely needed because human error is a huge threat to your organization, and if we can prevent an attack with user education, it's a huge win for everyone. No technical solution is needed. We offer phishing training along with all the usual attack scenario training. IdAM—identity & access management is another core solution needed by every organization because you should assume the hackers have your password—either from a previous breach or because it can easily be cracked. Since passwords are dead, there must be a second factor to protect user accounts.

**TAG Cyber: Do you have any predictions about whether securing SMBs can play a role in future global cyberwars?**

**CYVATAR:** Let's face it, most businesses are SMBs. What this means is that their attack surface is huge, and many of them don't have robust security programs. This makes them ripe for cyberattacks. SMBs are just low hanging fruit. So, if there's a major cyberwar, they will get hit first and may be used as a pathway to larger companies they may have access to, as in the Target breach.

---

**A cyBer Security class Somewhere in New Jersey:**



*“Do whut I say and yer bad emails will sleep with the phishes.”*



AN INTERVIEW WITH HENRY HARRISON,  
CO-FOUNDER & CSO, GARRISON TECHNOLOGY

# BROWSER ISOLATION AS A KEY ENTERPRISE SECURITY CONTROL

It's quite jarring to see the types of potentially dangerous content that finds its way onto an endpoint when the user is browsing a typical website. To address this challenge, isolation methods have emerged that separate the browser from the endpoint via solutions that run either in the cloud or a data center.

Garrison has been a leader in the browser isolation market, offering solutions that depend on hardware and can be delivered either on-prem or as a cloud service. We wanted to gain a deeper understanding of how this would work in a typical enterprise.

***TAG Cyber: What is the threat to the endpoint from content-rich websites?***

**GARRISON:** The threat to organizations from the web is vast, and web-borne attacks such as ransomware and phishing are all too common. In fact, the FBI last year reported an increase of over 400% in phishing attacks. Additionally, Google Safe Browsing lists just under 2.1 million websites as dangerous. And Google's list only includes the dangerous websites we know about. The unknown threats could be far greater in number. Currently, enterprises are having to deal not only with a huge increase in the number of attacks, but also in the cost of dealing with them. And although user training and other security controls can help, ultimately in the face of such an onslaught of targeted, sophisticated threats, it's a real uphill battle. Organizations can choose to block large proportions of the web to protect themselves, but this poses a real challenge from a business perspective.

***TAG Cyber: How does the Garrison solution work?***

**GARRISON:** Web Isolation solutions work by effectively removing the browser from the endpoint, running it instead in a completely isolated environment and relaying the browsing session back to the user. There are a number of ways to deliver Web Isolation, but Garrison uses a technique called pixel-pushing to transform all web content consumed by the user into a guaranteed safe format (pixels). We do this using custom-designed hardware, deployed as a cloud service, which allows us to benefit from hardware acceleration in order to offer a great price/performance ratio. Our hardware includes

**Our cloud offering uses the same hardware-based Web Isolation technology, but deployed in the cloud rather than in customer data centers. It was built from the ground up for multitenancy and is operated by Garrison rather than the customer, removing the management burden of an on-prem solution.**



gigabits of video compression silicon so that we can take the guaranteed safe format—raw pixels—and deliver that in real time over real-world networks.

The hardware design also allows us to deliver exceptional security. Indeed, our security is good enough for some of the most demanding military and national security customers in the U.K., U.S. and other allied nations. Unusually, the level of security we're offering may actually be more than most of our commercial customers really feel they need; but at the level of price/performance we can deliver, that extra level of security effectively comes for free.

***TAG Cyber: How do you provide a hardware solution as a cloud service?***

**GARRISON:** Our cloud offering uses the same hardware-based Web Isolation technology, but deployed in the cloud rather than in customer data centers. It was built from the ground up for multitenancy and is operated by Garrison rather than the customer, removing the management burden of an on-prem solution.

***TAG Cyber: Tell us more about the pros and cons of using hardware as an isolation control.***

**GARRISON:** In terms of pros, hardware has many benefits from a security perspective. First, it's much harder to exploit hardware than software, which is by its nature inherently vulnerable. Garrison uses hardsec technology (particularly the use of Field Programmable Gate Array silicon—FPGAs) to deliver the security functions of the product, meaning it is secure enough to be trusted by some of the most security-sensitive organizations on the planet. But crucially for our commercial customers, delivering pixel-pushing Web Isolation using hardware rather than software has the added benefit of allowing us to deliver a solution that is highly scalable and highly usable at a very competitive price point.

Historically, using hardware had its drawbacks, as this meant delivering a solution on-prem that can come with challenges in terms of deployment and management. However, being able to deliver this as a cloud solution resolves this challenge. Of course, from an engineering and product development perspective, building a hardware solution is definitely more of a challenge! However, Garrison has assembled a world-class engineering team that has now more than proven its ability to deliver.

***TAG Cyber: Do you have any predictions about whether browser isolation can play a role in future global cyberwars?***

**GARRISON:** In many areas, this type of isolation technology already plays a role in the existing global cyberwars, as evidenced by some of the military and national security organizations using these solutions today to protect their most sensitive systems and data. The real question is whether it becomes increasingly appropriate to describe as “cyberwar” the threat landscape faced by civilian and commercial enterprises—particularly those providing critical infrastructure. If that’s the future that we face, then it simply won’t be sustainable to provide broad-based web access as we do today, which essentially invites people we don’t know to send arbitrary code to execute on our users’ endpoint devices.

---



*"Welcome to The CISO Show! Each week, you  
our audience members can win big prizes  
by guessing the exact dates when these CISOs  
will be fired!"*



AN INTERVIEW WITH ZIAD GHALLEB,  
PRODUCT MARKETING, GITGUARDIAN

# SCANNING GITHUB FOR VULNERABILITIES AND SECRETS

Software development teams now understand the value of security solutions for their coding platforms. The DevOps process is now typically integrated with controls that attempt to detect and remediate vulnerabilities or secrets that might be exploited by external hackers or compromised insiders with authorized access.

GitGuardian supports this objective with a commercial platform that scans GitHub, GitLab, and Bitbucket by Atlassian to detect and remediate potential security issues or secrets that might be exploited. We wanted to gain deeper insight into how its solution is used.

***TAG Cyber: What are the primary threats to DevOps?***

**GITGUARDIAN:** The primary threats come from within. The shortening of release cycles and the focus on continuous delivery to production environments are not without any risks. Speed and automation are a double-edged sword. While DevOps allows for the faster delivery of value to customers and end users, it also gives rise to previously unseen security challenges such as cloud infrastructure misconfigurations, code tampering and leakage, vulnerable workload containerization and more.

In addition, developers and DevOps engineers, essential to operating the DevOps lifecycle, are increasingly becoming targets in sight for hackers. Humans can be the weakest link in any system, and DevOps is no exception. Granting over-provisioned access for developers to environments and credentials is another major risk security teams should consider.

***TAG Cyber: How does the use of GitHub create potential vulnerabilities?***

**GITGUARDIAN:** There are many ways in which using GitHub can cause headaches for organizations and their security teams. For context, GitHub is the largest code-sharing platform with more than 50 million developers and 60 million hosted repositories. Our research in this space has led us to scan more than a billion code commits every year, and we have uncovered many interesting findings. Developers like to tinker with open source and personal projects in their free time. It gives them a break from the professional setting to express

## Organizations deploy GitGuardian Internal Monitoring with a primary use case in mind: reducing the risk of exposure of their secrets (API keys, tokens, database credentials...) in the first place.

unbounded creativity and learn new technologies. But there's a caveat. Security-wise, the access model to SaaS-based version control systems like GitHub is fundamentally flawed. It is usually granted through personal emails, which developers use to log in and contribute to all sorts of projects—professional, personal and open source—all from a single account.

We found these **multipurpose accounts** to be the source of many vulnerabilities. Our full-scale public GitHub repositories scan returned volumes of corporate secrets and sensitive data, many of which were exposed in the personal public repositories of developers. For organizations, such threats lie far beyond the reach of their traditional monitoring tools, let alone the control of their security policies. We also found fragments of proprietary source code, ranging from technical interview questions to sensitive cloud infrastructure configurations, publicly leaked on the same personal repositories and accessible by any user of the GitHub platform!

To learn more about our research on public GitHub, Docker Hub and private code repositories, read our recently published report, [The State of Secrets Sprawl 2022](#).

### ***TAG Cyber: How does the GitGuardian platform work?***

**GITGUARDIAN:** Our Internal Monitoring automates secrets detection and remediation throughout the software development lifecycle (SDLC). The GitGuardian platform plugs into the DevOps tools and infrastructure (VCS, CI/CD tools, IaC configurations) that make up the software delivery pipeline, giving application security teams the visibility they need and the power to enforce consistent security policies across the organization. The platform continuously scans the SDLC for policy breaks or vulnerabilities such as secrets-in-code. When incidents are raised, GitGuardian will deliver alerts to security engineers and trigger automated remediation workflows. The developers involved receive invitations to team up with security or resolve their incidents by themselves, effectively reducing the burden put on application security engineers.

### ***TAG Cyber: Tell us more about the type of use cases most common for your platform.***

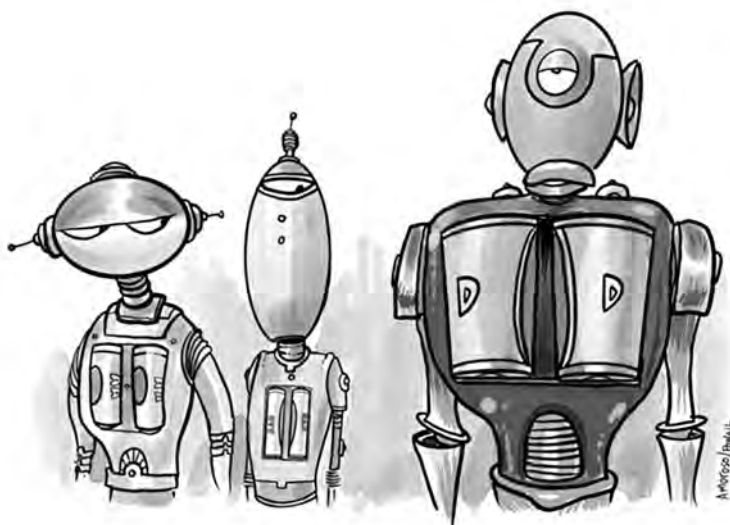
**GITGUARDIAN:** Source code moves across many different tools and teams, making it difficult to keep track of in the development lifecycle. If it leaks, the hardcoded secrets it may contain will give attackers effortless access and allow for lateral movement and deeper penetration into an organization's IT systems. Organizations deploy GitGuardian Internal Monitoring with a primary use case in mind: reducing the risk of exposure of their secrets (API keys, tokens, database credentials...) in the first place.

And the platform helps them reach this goal thanks to a layered approach to security, covering every stage of the software development lifecycle.

First, by connecting to all the tools that make up the SDLC, GitGuardian gives security teams an overview of incidents and policy breaks across time and space. Second, by scanning Continuous Integration pipelines, GitGuardian automates security testing and contributes to aligning DevOps engineers with their security counterparts. Finally, by providing developers with command-line applications (CLI) to scan their contributions for vulnerabilities, GitGuardian enables Shift Left security and reduces the accumulation of security debt starting from the first line of code. In the process, organizations will also find themselves achieving compliance with frameworks such as NIST Recommended Minimum Standards for Software Testing and, more importantly, instilling a DevSecOps culture where security is a shared responsibility.

***TAG Cyber: Do you have any predictions about whether DevOps security can play a role in future global cyberwars?***

**GITGUARDIAN:** DevOps security appears to be a significant departure from the traditional paradigms of cyberwarfare. But the past is never a good predictor of the future, and what worked for previous hacks may never work again, so I would like to say there will definitely be a role for DevOps security in this context.





AN INTERVIEW WITH PAUL AYERS,  
CO-FOUNDER & CEO, NOETIC CYBER

## CONTINUOUS MANAGEMENT OF CYBER ASSETS AND CONTROLS

The challenge of identifying and managing assets in the context of cybersecurity has grown considerably in recent years, especially for companies with a non-trivial set of complex resources. As such, teams must find ways to observe and manage their assets continuously to deal with the growing risk to enterprises from malicious adversaries.

Noetic provides a commercial platform designed to continuously manage cyber assets and controls across an enterprise. We wanted to learn more about how such foundational support can reduce cyber risk.


**TAG Cyber:** *What is the issue with identification of assets and controls? Why is this so difficult?*

**NOETIC:** This is, in part at least, a problem of scale. The digital transformation that we've all experienced over the past few years has resulted in extraordinary technology sprawl. At one point, security and IT organizations could impose restrictions on the adoption of new applications and the roll-out of devices. Today that is impossible. This is the result of major global trends around the adoption of cloud services and SaaS applications, the "democratization" of IT buying and the very nature of how we live and work today. So, we need to think about assets differently. Traditionally, the word "asset" implied a compute device, but we now think of assets as anything that has a cyber impact on the organization. It could be a vulnerability, a person, a network, a policy, and all these assets are interconnected. The cyber relationships between them are how we understand and measure risk.

Organizations need to understand what assets they have, but more importantly they need the relevant business context to know why they should care. A vulnerability is not important by itself, but if it's present on an internet-facing machine with access to share price-affecting systems, then that's different. Controls are part of the same problem. We layer frameworks on top on untrustworthy data, so we have no real level of assurance. This is a major inhibitor to building modern cybersecurity processes, such as zero trust. At a basic level, by not knowing what we have, we can't properly understand and mitigate cyber risk.



Attackers are constantly scanning our external attack surface to find unprotected assets, and we need a dynamic, continuous approach to find our security coverage gaps before they do.



***TAG Cyber: How does the Noetic platform work?***

**NOETIC:** The Noetic platform is based on the idea that organizations have enough tools. The problem they have is that all that relevant data is siloed in different IT, DevOps and security platforms that don't have the necessary context or shared understanding to make use of it.

We wanted to take the "gold" from all these systems and use it to build a model of all assets in the organization—how they relate to each other, and what cyber risk they bring. To do this, we looked outside of traditional cyber tactics to see what innovative approaches were being adopted to manage and analyze large data volumes and we've brought that back to cybersecurity.

The two main developments that have allowed Noetic to deliver this visibility are modern API frameworks and graph databases. By using OpenAPI templates, we can quickly integrate with most IT and security tools, using their data to get specific perspective on the asset landscape. We then aggregate and correlate the data across all the tools and build a model of it in a graph database. Graph is important here as it allows us to understand these cyber relationships and add context to the data in a way that wasn't possible before. That correlated data model supplies new insights to the security team based on context and criticality. What machines are missing vital security controls? How do we prioritize vulnerability management and patching based on business criticality? Which high-risk applications are missing multifactor authentication (MFA)? These insights help security teams understand their cyber landscape and partner better with IT and DevOps because everyone can now work on the same shared understanding of cyber risk. But we also believe that visibility is only half of the story. Security teams need these insights to be actionable.

At the core of the Noetic platform is a comprehensive automation and workflow engine. My co-founders and I had pioneered the Security Orchestration, Automation and Response (SOAR) market at our earlier start-up, Resilient Systems. From that experience, we understood the power of automation—but also its limitations. For automation to be truly effective for cybersecurity use cases, it needs certainty. Once we understand cyber posture gaps, or control problems, we can then use automation to correct them, which is critical to meeting the scale and speed needed in the modern enterprise.

***TAG Cyber: Why is continuous and on-going asset management such an important issue?***

**NOETIC:** Continuous is the critical word here. If we look at many areas of computing, we've seen a transition in recent years from



a static to dynamic approach. Automation is being adopted across our industry to meet customer demand and scale, and cybersecurity is no exception. Modern computing is increasingly ephemeral. Systems and containers are created for a specific task and then spun down. But just because they only exist for a brief time doesn't mean they don't present a risk to the business. Attackers are constantly scanning our external attack surface to find unprotected assets, and we need a dynamic, continuous approach to find our security coverage gaps before they do.

Good cyber asset management is also a foundational element of any cybersecurity strategy. It's first on the list in the CIS controls framework and in NIST's guidance on migrating to a zero trust architecture, where they are clear that it "requires an organization to have a detailed knowledge of assets." So, we see continuous cyber asset management as a critical first step in any security transformation process, and one that is getting more attention from cybersecurity leadership. There's a growing realization that we need to tackle some of the fundamental cybersecurity challenges across the industry to get out of the vicious cycle we are in today, where teams are just focused on responding and remediating security incidents and can't take the learnings from them to focus on overall cyber improvement.

***TAG Cyber: Tell us more about the types of use cases most common for your customers.***

**NOETIC:** One of the key values of a cybersecurity asset management platform is the flexibility it can provide to support a wide range of use cases, and we have made sure to build in that extensibility to adapt to different scenarios, but there are common challenges we see across our customers. The first would be around security coverage gaps. Missing EDR or device management agents on virtual or physical machines is a common one, as is gaps in the vulnerability scanning process. These can be quickly found and addressed, and automation works well here to continuously enforce the desired policy. Vulnerability Management is another important use case. Mapping assets, vulnerability data and business criticality help security teams to understand which vulnerabilities require immediate attention as opposed to the general backlog. Many of our customers have found CISA's known exploitable vulnerability database to be an incredibly valuable resource here, and we're providing that information integrated in the platform, as well as insights from NIST, MITRE and more. The tool also plays an important part in supporting the Incident Response process. SOC analysts can gain important context when they are conducting an investigation by querying incident data and uncovering previously unknown links to other assets.



## AN INTERVIEW WITH CAMERON GALBRAITH, DIRECTOR OF PRODUCT MARKETING, NONAME SECURITY

# PREVENTING ABUSE OF APIs

---

As businesses come to depend more on their APIs as the foundation for their missions, the problem emerges of dealing with malicious fraudsters. The abuse of business logic through APIs, for example, can create security vulnerabilities which in turn can have serious consequences to the organization.

Noname Security is a leading commercial solution provider addressing these API security objectives for enterprises. We wanted to learn more about how the Noname API Security Platform reduced API security risks for modern enterprise teams.

### ***TAG Cyber: What types of threats exist today for APIs?***

**NONAME SECURITY:** APIs are the lifeblood of digital transformation. “Cloud” and “apps” are just code words that mean “lots and lots of APIs.” Business critical applications and data now all run on APIs, which means it’s more imperative than ever to protect APIs from any type of vulnerability—from simple misconfigurations to a full scale attack.

Unfortunately, API threats are all too common. They’re on the rise, costly and time-consuming to remediate. Most enterprises lack the visibility and discoverability necessary to even detect a threat. For example, most don’t know how many APIs they have, which APIs are communicating sensitive information, or even who or what the APIs are communicating with. And traditionally, once a compromise is detected, it can take months to determine the root cause of a data leak or attack to remediate. All the while, applications and environments are constantly evolving. New changes are introduced for existing APIs, and new APIs are being deployed faster than they can be secured.

### ***TAG Cyber: How does the Noname platform work?***

**NONAME SECURITY:** The Noname API Security Platform protects APIs in real-time and detects vulnerabilities and misconfigurations before they are exploited. The platform is an out-of-band solution that integrates with your existing infrastructure and spans across three core capabilities:

API Security Posture Management allows users to inventory every API, including legacy and shadow APIs, with automated data classification

Because APIs are used by every corner of the business, it was important for us to design a solution that supported the entire API lifecycle and delivered value to each along the way, from developers to operations to security.



security posture details. API security analytics flags high risk misconfigurations and API security vulnerabilities in policy and specs, so that AppSec teams can prioritize remediation efforts.

API Runtime Security offers AI and ML-based models for runtime API threat detection. Then there's automated and semi-automated blocking and threat remediation.

"Shift Left" with API Security Testing features automated and dynamic API security testing for CI/CD pipelines. Users can continuously test APIs to identify security risks before they emerge.

***TAG Cyber: How do you weave your solution into the modern DevOps process?***

**NONAME SECURITY:** Because APIs are used by every corner of the business, it was important for us to design a solution that supported the entire API lifecycle and delivered value to each along the way, from developers to operations to security. The Noname API Security Platform embraces "Shift Left" and identifies performance and security issues early in the development process, identifies configuration issues and vulnerabilities within policies and specs through deployment, and provides threat detection and remediation functionality in the runtime.

***TAG Cyber: Tell us more about the most typical use-cases for your product in operation.***

**NONAME SECURITY:** The interest in our solutions evolves as the relationship grows. Most companies are aware that they have blind spots within their API estate and are interested in discovery and posture management. However, once we turn the lights on, we usually find a significant amount of issues, and an inventory of APIs much larger than the client anticipated. The runtime security and active testing capabilities then become the most typical use cases— protecting the environment from any kind of threat and ensuring the validity and integrity of all new and existing APIs.

***TAG Cyber: Do you have any predictions about whether API security can play a role in future global cyberwars?***

**NONAME SECURITY:** It's not the future of global cyberwars, *it's already upon us.* Digital transformation and cloud migration initiatives are API-first. The industry is quickly headed to an API-only world and that means the volume and severity of API threats will only increase. We see it in the news every week. It's crucial for enterprises to eliminate their API security blindspots and implement API security platforms and processes that can operate at the speed and scale of their business.



AN INTERVIEW WITH LARRY HURTADO,  
MANAGING DIRECTOR U.S.A., QNEXT CORP.

## EXTENDING ZERO TRUST DATA ACCESS TO THE ENTERPRISE

Every security expert agrees on the power of zero trust for network and application access across the underlying network infrastructure. But the use of zero trust tooling to support secure access directly to files and folders has only recently become possible.

Qnext is now offering a zero trust data access (ZTDA) solution called FileFlex that supports secure data access objectives. We were interested to learn more about how this platform can be deployed effectively.

***TAG Cyber: What is zero trust data access and how does it relate to networks and applications?***

**QNEXT:** Zero trust data access describes microsegmented access to files and folders using a zero trust architecture. The zero trust paradigm assumes an enterprise has been breached and works to mitigate the negative impact of the breach through identity verification (user and/or device authentication, microsegmentation, and policy-based least privilege access). Zero trust data access differs from zero trust network access in that the latter describes authorized access to a network segment or device, but by default allows access to all applications and data on any server on that network segment. And zero trust data access differs from zero trust application access in that it describes authorized access to applications, but by default allows access to any data or file that is controlled by that application.

***TAG Cyber: How does the FileFlex platform work?***

**QNEXT:** The FileFlex Enterprise platform uses a unique patented architecture comprised of three main components: FileFlex Enterprise server (and PKI server); FileFlex Enterprise Connector Agent; and FileFlex Enterprise Client App. All are required to make the solution work.

Together they work like a bank teller. When you go to a bank, you are not allowed to enter the vault to get your money yourself. You have to see a bank teller who will check your identity, see if you have the money, and then check that you are allowed to withdraw it. If everything checks out, the teller communicates with a second teller inside the vault. The vault teller gives the money to

One of the unique differentiators of FileFlex Enterprise: It is the first and only platform that brings remote access and sharing to an entire IT infrastructure of on-premises, cloud-hosted and SharePoint unstructured data storage and puts it under a single pane of glass.



your teller, who then gives it to you. That's how the bank secures access to money. In the same way, if you want to remotely access or share files in the organization's storage infrastructure, you can't just go into the infrastructure and get them. FileFlex uses its zero trust architecture to verify your identity, then check your request against policies set for you. If everything is OK, then the server contacts the connector that sits behind the firewall. The connector acts as a proxy to get the permitted file, encrypt it and send it to you via the server. Users don't have direct access, they have visibility and access only to storage that is permitted by policies. Remote access and sharing of files and folders are protected by identity verification, policy and role-based access, microsegmentation, and least-privilege access.

***TAG Cyber: How do you provide support for secure access to existing enterprise resources such as SharePoint?***

**QNEXT:** FileFlex supports existing enterprise resources, on-premise servers, server-attached storage, network-attached storage and PC via the FileFlex Connector agents. They are a software-only component that runs on a device located on the corporate infrastructure behind the corporate firewall. The FileFlex Connector agent can access any device or storage located on the same infrastructure, on behalf of the user, using local permissions. The main purpose of the FileFlex Connector agent is to perform the requested task (access, relay and manipulate data) located on the same infrastructure, on behalf of a user as if the user were physically present on that infrastructure. The FileFlex Connector agent is also responsible for encryption and decryption functions for all data transmissions, as well as managing revisioning and aspects of collaboration functions.

Additionally, as a pure-play Zero Trust Data Access (ZTDA) provider, we make professional services available to those organizations desiring greater levels of support to help further accelerate an organization's transition to a full zero-trust network. The combination of our FileFlex Enterprise platform and our Professional Services offerings enables organizations to reduce security risk at a pace that aligns with the security risk tolerance of the organization's board.

***TAG Cyber: Tell us more about how your solution would work across complex enterprises with cloud and IaaS-hosted assets?***

**QNEXT:** One of the unique differentiators of FileFlex Enterprise: It is the first and only platform that brings remote access and sharing to an entire IT infrastructure of on-premises, cloud-hosted and SharePoint unstructured data storage and puts it under a single pane of glass. This includes your public clouds such as Dropbox, Google Drive, OneDrive and Box, as well as private clouds and Infrastructure-as-a-Service clouds such as Microsoft Azure, Amazon S3 and Google Cloud.

***TAG Cyber: Do you have any predictions about whether zero trust data access can play a role in future global cyberwars?***

**QNEXT:** Today all organizations are worried about ransomware attacks. We have a massive remote workforce using a multicloud hybrid-IT storage infrastructure. Now as much as 80% of corporate data is unstructured. Organizations are finding it increasingly difficult to govern remote data access and manage and protect their many unstructured data repositories. And unstructured data is the primary entry point for malware and ransomware.

FileFlex Enterprise is an overlay service that blankets an organization with a zero trust data architecture for remote data access and sharing. It uses the zero trust architecture to allow remote workers and contractors to share data seamlessly and thereby reduce risks associated with ransomware due to more secure remote access to unstructured data. With the FileFlex zero trust data architecture from the ground up, every data request is verified using corporate access policies including LDAP and Active Directory and most leading technology and identity management providers. The granular, real-time event log provides your IT team full audit and access visibility with alerts. Least-privilege access and microsegmentation control remote data access protecting corporate data against malicious actors. All of this allows FileFlex Enterprise to address security problems with external contractors, your B2B supply chain and partners.



***“I don’t need your driver’s license number.  
I just pulled it up on Tik Tok.”***



## AN INTERVIEW WITH LIRAN TANCMAN, CO-FOUNDER & CEO, REZILION

# SECURING CODE DURING DEVOPS

---

The goal to secure code during DevOps is a major objective for modern enterprise teams who create and use software. This requires a variety of automated tasks including the ability to ensure that code comes from trusted repositories, to validate that all vulnerabilities have been removed and to generate a deep understanding of the code through workload compositional analysis.

Rezilion is a DevSecOps platform that helps customers eliminate software vulnerabilities across cloud workloads, applications, and IoT devices, empowering developers and security teams to accelerate innovation without risk. We were interested to learn more about how the Rezilion solution worked in a typical software development process.

***TAG Cyber: What is the biggest challenge to securing code?***

**REZILION:** The biggest challenge to securing software code is identifying and remediating what is truly exploitable. Digital transformation initiatives are driving organizations to innovate and release products faster, and that causes a growing vulnerability backlog. Developers don't have the time or tools to fix every vulnerability fast enough to meet security and compliance requirements. Yet, at the same time, the security team must ensure that products don't contain dangerous vulnerabilities that could be exploited and put the organization at risk.

***TAG Cyber: How does your platform work?***

**REZILION:** Ours is an end-to-end DevSecOps platform that identifies, prioritizes and reduces your vulnerability backlog by over 70%. The platform ensures quick results by helping customers remediate in days, not months. Rezilion uses a proprietary static and dynamic enhanced run time analysis to identify vulnerabilities that are loaded into memory, and thus exploitable, and those that are not loaded to memory, and therefore pose no risk. Enhanced granularity of the exploitable vulnerabilities further helps to prioritize what to remediate first. The Rezilion platform also provides a comprehensive and continuous dynamic software bill of materials that affords a real-time view into the actual attack surface.

***TAG Cyber: How do you determine the types of repositories from which the code is generated?***

**REZILION:** The platform ensures that only code from trusted sources can run in production by certifying the repositories and processes responsible for promoting them into runtime. The certification enforcement is driven by customer-







AN INTERVIEW WITH ITZIK KOTLER,  
CO-FOUNDER & CTO, SAFE BREACH

# USING BREACH AND ATTACK SIMULATION TO REDUCE CYBER RISK

The breach and attack simulation (BAS) method is well-established for enterprise security teams as an effective method for cyber risk reduction. The key issue now is whether a given BAS solution works accurately and integrates smoothly into the enterprise environment.

SafeBreach is a leader in the BAS field, with much experience serving enterprise teams in all sectors. We asked them to share how their platform has evolved in recent years.


***TAG Cyber: What is meant by breach and attack simulation (BAS)?***

**SAFE BREACH:** BAS tools can effectively help security teams prepare for cyber threats. However, not all BAS tools are created equal. SafeBreach offers a powerful and versatile tool that allows security teams to safely execute a variety of realistic and advanced attacks against their security controls to gain visibility into security gaps. As a result, they are able to improve the efficacy of the security operation center (SOC) by reducing the mean time to detect (MTTD) and mean time to respond (MTTR). When helping prepare for a ransomware attack, SafeBreach offers a host of unique, built-in capabilities that enable security teams to understand the scope and nature of the attack by thinking like the attacker. In 2021 alone, SafeBreach added 120 new attacks identified in US-CERT and other high-profile alerts, including several new malware, zero days and critical vulnerabilities. Another 78 were ransomware-specific attacks in 2021. These scenarios provide templates to create and run tests that cover prevalent attacker behaviors that may lead to cyberattacks on organizations.

***TAG Cyber: How does the SafeBreach platform work?***

**SAFE BREACH:** We are the industry's only breach and attack simulation application that uses correlative analytics to identify security gaps and link them to their potential business impact. This is a key differentiator between SafeBreach and other BAS platforms. While others solely examine attacks at the individual level, we correlate data from a large number of simulations to generate a priority-based set of recommendations.

Customers can see at which phase of an attack they are most vulnerable and which tools they employ leave gaps for attackers to take advantage of.



SafeBreach's "Hacker's Playbook" is the largest, most detailed, and most up-to-date compendium of programmatically accessible exploits and known attack types in the world, with over 20,000 breach methods, all of which can be run by SafeBreach's system on a continuous basis without impacting an organization's assets or networks. Our lab is dedicated to tracking the industry and updating the playbook based on government alerts within 24 hours. This is a strong competitive advantage. Data from our validations can improve SOC team responses and empower management teams to better manage risk and invest resources. SafeBreach enables data-driven risk analysis, resource prioritization and guided mitigation. The platform continuously and safely tests and optimizes the effectiveness of your security infrastructure against the business value of your assets and helps security teams ensure their security controls and processes are effective against real world attackers by continuously challenging them.

SafeBreach's vision is to transform the way the industry validates security to enable security teams to understand and reduce risk continuously, from static to continuous, from theoretical to practical, from risky to safe. After all, when companies know which security controls actually work in their environment, they can invest for real impact and protect more. They can quantify risks to the business and drive a security strategy aligned with the company's business growth. What SafeBreach does—validate security controls continuously—changes the mindset of defenders to be offensive and proactive, and the end result is that we help to build a safer world.

***TAG Cyber: How do your customers integrate the platform into their overall security validation program?***

**SAFEBREACH:** Our platform allows businesses to crash-test their networks to find the holes in their security stacks while simultaneously optimizing customers' spend on cybersecurity. With our BAS technology, businesses can test their security tools against thousands of attack methods included in our hackers' playbook. Customers can see at which phase of an attack they are most vulnerable and which tools they employ leave gaps for attackers to take advantage of. As customers run through these simulations, they also receive validation (or lack thereof) that their security tools are working as they should be. SafeBreach will identify tools that aren't working properly, and thus provide the CISO and buyers with insights into where their investments are paying off and where they're burning a hole in their wallets. Through its integrations with a wide variety of technology partners, SafeBreach unifies people, processes and technologies and helps security teams understand the real risk to the business and improve overall SOC process efficiency. Yes, time is money... but so is money. And SafeBreach ensures it's invested in the right

places. We provide a holistic view of an enterprise's security posture, allowing key stakeholders to make informed security decisions to protect themselves against an ever-changing threat landscape.

***TAG Cyber: Tell us more about the output from your platform and how it can be used to make decisions about cyber risk.***

**SAFE BREACH:** We help security teams ensure their security controls and processes are effective against real world attackers by providing an automated way to reduce the risk of future breaches. We have a 24-hour SLA for US-CERT alerts which enable our customers to operate quickly. This information becomes part of the Hackers Playbook. This broad visibility enables us to deliver actionable guidance on mitigating your risks and prioritizing your resources. Using SafeBreach to prepare against ransomware or other malware attacks can provide immediate value with a clear business impact, including the ability to understand the efficacy of existing security stacks, identify gaps, reduce risk, inform budgeting decisions and support alignment across the company.

***TAG Cyber: Do you have any predictions about whether BAS solutions can play a role in future global cyber wars?***

**SAFE BREACH:** Cyber is asymmetrical warfare. The defenders need to protect 100% while the attackers need to succeed only once. BAS technology levels the "playing field," so to speak, by allowing the defenders to see some of the techniques the attackers can use and simulate it ahead of the time.



*"Now let's talk about this work obsession of yours."*



## AN INTERVIEW WITH ROEY ELIYAHU, CO-FOUNDER & CEO, SALT SECURITY

# REDUCING CYBER RISK FOR MODERN APIS

The application programming interface (API) has emerged as the primary means by which companies access services dynamically to support their mission. Because of their role in sharing valuable data and services, APIs have emerged as a primary attack surface, as we've seen from headlines about API security incidents. Developers are coding fast, and APIs can be complicated, with wide variance in design and implementation. The resulting vulnerabilities can make it easier for bad actors to find a way in.

Salt Security is a prominent provider of API security solutions. We were eager to better understand the technical approach Salt takes to reduce API risk.


### ***TAG Cyber: What are the cyber risks to APIs?***

**SALT:** APIs are built expressly to connect applications to sources of data and to each other. Companies are using more APIs than ever, and those APIs are more functional than ever. Hackers have figured out that targeting APIs is lucrative. Often they find a gap in business logic that they can exploit, and existing security technology isn't architected to identify the reconnaissance activities of hackers looking for mistakes.

### ***TAG Cyber: How does the Salt platform work?***

**SALT:** The Salt Security API Protection Platform protects APIs across the entire API lifecycle. We identify vulnerabilities in the development phase, before any security gaps can be exploited, and we provide runtime protection to protect APIs already in production. Our platform connects into customers' environments and gets a copy of the API traffic. We can leverage more than 60 different ways to integrate, across all application types, with nothing deployed inline so we can't impact application performance. We feed that mirrored API traffic into our API Context Engine, which baselines all behavior across millions of users and API calls simultaneously, building rich context of what's "normal" in each customer's environment. Only Salt provides cloud-scale big data to detect API attacks. Since these attacks unfold over days, weeks and even months, you need the scale of the cloud to stitch together attacker behavior over time. On-premises solutions simply cannot store enough data to identify today's sophisticated API attacks. We use our API Context Engine to discover all APIs and the sensitive data they expose, pinpoint and stop attackers, and identify pre-production and runtime vulnerabilities. Then we share the remediation details developers need to harden

Hackers have figured out that targeting APIs is lucrative. Often they find a gap in business logic that they can exploit, and existing security technology isn't architected to identify the reconnaissance activities of hackers looking for mistakes.



APIs. Because we're not inline, we connect into our customers' existing inline devices, like gateways, WAFs and load balancers, to block attackers.

***TAG Cyber: How do you work with developers to ensure that the Salt platform integrates smoothly into their API environment?***

**SALT:** Our platform helps developers improve the security posture of their APIs in a number of ways. For pre-prod APIs, our API design analysis leverages OAS or Swagger documentation to identify vulnerabilities based on the code design. Our API drift analysis runs test traffic against pre-prod APIs and compares the results to documentation to see where API design and execution have diverged. The platform can also simulate attacks, further helping to identify vulnerabilities or business logic gaps in the APIs before releasing them into production. In all these cases, the Salt platform can integrate with CI/CD systems as stringently or loosely as dev teams prefer. We can send alerts on vulnerability findings directly within the CI/CD system, or we can design it to fail a non-compliant build. Organizations have the choice of how tightly they want to enforce API design controls.

***TAG Cyber: Tell us more about how Salt can be connected to other aspects of the enterprise security environment?***

**SALT:** Beyond the more than 50 agentless ways to integrate into a customer's environment, and the CI/CD integrations, the Salt platform can also tie into Slack, Jira, ServiceNow, PagerDuty or any other ticketing system to send remediation insights to the developer. It ties into Splunk, or Sumo Logic or any other SIEM to share API incident reports with SecOps teams. We also integrate into Snowflake for data analysis, and customers use our webhooks option to integrate Salt into any workflow in their company.

***TAG Cyber: Do you have any predictions about whether API security can play a role in future global cyberwars?***

**SALT:** I created Salt because when I was engaged in white hat hacking as part of cyber defense for Israeli military and government systems, I routinely found APIs the easiest place to break into a system. Look how quickly state hackers exploited the Log4j vulnerability to attack systems. I have no doubt bad actors around the world have set their sights on APIs as the weakest link in many of the systems they're looking to attack. Consider how many headlines we saw in 2021 about API security breaches—and those were just the incidents that became public. Cyberattacks targeting APIs are definitely already running in full force. It's just too easy to find holes in the system.



AN INTERVIEW WITH RITA GUREVICH,  
FOUNDER & CEO, SPHERE TECHNOLOGY SOLUTIONS

## ADVANCING CYBER HYGIENE FOR ENTERPRISE

---

Few aspects of the modern enterprise require as much attention as attending to basic cyber hygiene. With malicious attacks increasing in both frequency and consequence, companies now feel the urgency to immediately attend to basic tasks such as cleaning up permissions to secure their valuable assets.

SPHERE is addressing this cyber hygiene challenge with a range of commercial platform solutions. We wanted to learn more about the SPHERE approach, including how it is being used by enterprise teams today.

***TAG Cyber: What is meant specifically by cyber hygiene?***


**SPHERE:** When we speak about cyber hygiene, we are referring to the upkeep of end user permissions and privileged access. Initially, we were a consulting company brought in by customers to clean up their open, excessive and non-standard permissions across data, servers, applications, etc. At the time, we called our team “access control janitors.” However, we have advanced so far beyond that, and automated so much with our flagship solution, SPHEREboard, that it made perfect sense to describe it in a more elegant way: Cyber Hygiene. Also, the term reflects the recognition that hygiene is not a one-time clean-up, but rather is all-encompassing, and must be an area that organizations focus on maintaining every single day.

***TAG Cyber: How does the SPHERE platform work?***

**SPHERE:** Here’s an example. SPHEREboard simplifies the technical complexity of file hierarchies, group enumeration, identity correlation and access mechanisms to enable clients to focus on the core question: Who has access to what?

First, the solution collects a ton of metadata by pulling relevant information directly from the platforms that require analysis and remediation. The contextual and referential sources are also queried and correlated to programmatically make sense of the mountains of information. Next, the output is arranged into meaningful data, based on the client’s needs, to show

**For each identified risk, our solution provides detailed action steps and a list of stakeholders to be engaged to resolve the issue.**



ownership of data assets, correlation of identities across platforms, and logical groupings for access permissions. Then, our user-friendly platform displays the information in a digestible and customizable format to allow clients to easily understand the scope of the access hygiene issues within their environment, and how to prioritize them for remediation based on risk, impact and effort. Finally, the client's access environment is cleaned up and transitioned to an evergreen state using proprietary automation.

Going forward, SPHEREboard's intuitive platform will allow the client to feel empowered as they regularly evaluate their environment with the savviness and insight of an access hygiene veteran.

***TAG Cyber: How do you weave actionable intelligence into your solution?***

**SPHERE:** The entirety of our solution is oriented toward providing actionable intelligence to allow clients to easily remediate access issues in their environment. For example, through SPHEREboard, clients can easily navigate a comprehensive checklist for risk resolution. For each identified risk, our solution provides detailed action steps and a list of stakeholders to be engaged to resolve the issue. Additionally, SPHEREboard recognizes there is not a "one size fits all" approach for core access control governance. Instead, we provide numerous methods by leveraging information we've collected so that users can be flexible in their configuration. This allows the right owner to action the proper entitlement review and enable SPHEREboard to make the necessary changes efficiently and without the risk of business disruption.

***TAG Cyber: Tell us more about data quality and how this affects cyber hygiene.***

**SPHERE:** An effective cyber hygiene program requires reliable data. We often find this to be an issue with poorly executed, or incomplete implementations of, IAM systems. When numerous applications lack direct connections, accurate ownership and complete group membership, it's not possible to identify a comprehensive list of users or accurately assess discrepancies in user access. Without this information, it's not possible to effectively plan cyber hygiene activities, and this, in turn, may result in a false sense of security, failed audits, wasted effort and insecure systems.



**TAG Cyber: Do you have any predictions about whether data hygiene can play a role in future global cyberwars?**

**SPHERE:** The unfortunate reality is that ransomware is here to stay, and I think executives are starting to become more anxious about the potential fallout of not securing sensitive data and critical systems. These days, cyberattacks are widespread, and many different industries are susceptible, including recent instances in financial services, health care and energy, just to name a few. When these types of high-profile attacks occur, people often talk about cyber defenses such as vulnerability management, incident response and incident recovery. However, those are reactive solutions. Cyber hygiene is a proactive solution that, when implemented properly, is essential to limiting the risk of significant impact.



*"I'm sorry, Gladys - but your focus on PCI compliance was just too much for me."*



## AN INTERVIEW WITH DAVID MOVSHOVITZ, CO-FOUNDER & CTO, TRACKERDETECT

# APPLICATION DETECTION AND RESPONSE

---

Current application security mechanisms detect and protect against the exploitation of application layer vulnerabilities. However, the actual use of applications isn't monitored, which enables internal and external users—users who have legitimate application access—to use them in ways that may cause damage, whether intentionally or unintentionally.

TrackerDetect is a cybersecurity startup that offers unique detection of misuse, abuse and malice conducted in business applications by authenticated users. We wondered how its platform protects applications from human error and targeted abuse by malicious users.

***TAG Cyber: Why should we monitor what users do in business applications?***

**TRACKERDETECT:** There are plenty of excellent products that identify and protect against the exploitation of application vulnerabilities, but ultimately people are the most serious threat to business applications. TrackerDetect monitors what people do. Our solution assumes that all applications are perfect and have no vulnerabilities. We then ask risk and security officers whether they have full visibility into how their business applications are being used. Do they know when misuse, abuse or malice takes place? The answers we get are in line with market research, which is that it usually takes months.

***TAG Cyber: Why can't rule-based solutions effectively detect behavioral anomalies?***

**TRACKERDETECT:** Enterprises currently try to monitor user behavior and detect malicious activities with rules, but rules suffer from several deficiencies. Here are three. It's almost impossible to define all the allowed scenarios with rules, so rules usually define forbidden scenarios, which means they can only detect *known* forbidden scenarios. You've got to fully understand an application's business processes in order to write rules that apply to it, which is not trivial; and you have to do this for each of the many applications in your organization, and they're all just a click away. Finally, maintaining rules properly is labor intensive and takes time, but rules that aren't properly maintained generate endless false positives and an impossible signal-to-noise ratio. The bottom line is that rules are a 20th century concept, which is now simply outdated and very limiting.

Most solutions are based on rules, which in turn are applied to the entire community. We can't write a rule that will be applicable to everyone because there will always be people who have a good reason to behave a bit differently.

***TAG Cyber: What is a signal-to-noise ratio, and why is it typically a problem for rule-based detection?***

**TRACKERDETECT:** A problematic signal-to-noise ratio basically means you're experiencing a high rate of false positive alerts, or "noise." We often see customers suffer from alert fatigue due to a 98% rate of false alerts. Analysts just end up ignoring them. This happens because most solutions are based on rules, which in turn are applied to the entire community. We can't write a rule that will be applicable to everyone because there will always be people who have a good reason to behave a bit differently.

***TAG Cyber: Why has UEBA not been applied to application layer detection?***


**TRACKERDETECT:** The implementation of user and entity behavioral analytics (UEBA) has been based on standard infrastructure operations. However, there are no standard operations in business applications. Each application has its own set of operations, and implementing EUBA for all applications hasn't been done. But more importantly, EUBA is usually based on statistical analysis, such as analyzing the averages, standard deviations and medians of various operations. But do I have an "average" day? No, each day is a bit different. A focus on "average" or "median" is therefore ineffective. It generates both false positives (i.e., false alerts) as well as false negatives (i.e., suspicious activities go undetected).

***TAG Cyber: How can we accurately detect anomalies within and across applications?***

**TRACKERDETECT:** We do this with activity flows and sequencing. Cisco uses the same concept to detect network layer anomalies with NetFlow. Applications have been absent so far, because how do we normalize so many different ones? Activity flows provide us with the context required for detection based on sequences and sessions. We normalize with activity-based flows to detect anomalies in applications. We're now applying them to applications precisely because we've seen them effectively detect anomalies on networks.

Our activity flow model is ubiquitous; the actual meaning of each activity is irrelevant. Since each user has differing activity flows per application, TrackerIQ learns multiple profiles per user. A patent-pending clustering engine groups the user activity flows and generates profiles. These profiles are our foundation for accurate detection of anomalous activities. TrackerIQ also assigns a risk score to each anomaly so that we can prioritize detected anomalies.

Once we start looking, we find patterns. And the more data we have, the more repeatable the patterns. These patterns of normal activity-flow profiles can be used to detect anomalies in a very accurate way.



***TAG Cyber: How does your TrackerDetect solution work?***

**TRACKERDETECT:** TrackerDetect proactively uses application logs to detect anomalies and unknown breaches.

Our underlying technologies are based on unsupervised machine learning of user activity flows. These activity flows are then clustered into behavior profiles for individuals, as well as for cohorts of users. The learning is based on analysis of user sequences of operations. We look at which operations were performed; the order in which operations were performed; and the time intervals between the operations in the analyzed sequence.

If we were to analyze three or four months of my daily activity, we would find similar patterns: days dedicated to solving problems... days dedicated to writing specs... days I spend in meetings. Once we start looking, we find patterns. And the more data we have, the more repeatable the patterns. These patterns of normal activity-flow profiles can be used to detect anomalies in a very accurate way.

***TAG Cyber: Do you have any predictions about whether application detection will play a role in future global cyberwars?***

**TRACKERDETECT:** Cyberwars have mostly been about access and penetration of the infrastructure layer. However, in the future we will see a second stage of penetration, one that exploits business applications to achieve the attacker's goals. Attackers will impersonate application users to bypass the monitoring of enterprise networks and infrastructure. Three global trends are leading the market toward application detection. First, applications are increasingly cloud-based SaaS for good reason, but that often takes away the control organizations had on-prem. SaaS, in turn, enables a plethora of applications, ostensibly creating a longtail ecosystem of applications, making rules even more ineffective, while, at the same time, expanding an organization's attack surface as APIs opens it to third parties.



**ANALYST  
REPORTS**

# A MATURITY MODEL FOR ACCESS CONTROLS TO IMPROVE CYBERHYGIENE

EDWARD AMOROSO

---

A maturity model for managing entitlements toward improved cyber hygiene is offered in this technical report. Enterprise teams are urged to use the maturity model to challenge their own organization to improve its capability for all permissions, privileges, roles, and other entitlements used for end-user and privileged access to data, applications, and systems.

## INTRODUCTION

Cyber hygiene has emerged as an essential consideration for enterprise security teams, especially in the context of permissions management. Specifically, practitioners have come to value the need to get back-to-basics regarding the provisioning, maintenance, administration, and use of permission-related credentials. When these tasks are done sloppily, the organization is exposed to a wide range of exploits from both internal and external actors.

To address this potential weakness, enterprise teams have made significant investments of time, effort, and budget into modern identity and access management (IAM) systems, supporting tools, and personnel to manage the process. These IAM components help to address security control needs ranging from authentication to authorization, and they are often augmented with privilege access management (PAM) and related add-on tools.

One area, however, where enterprise security gaps remain involves the management of permissions. Over the past decade, it has become clear with one public breach after another that bad management of permissions has emerged as one of the most common root causes. Famous incidents such as the Colonial Pipeline situation, for example, included sloppy management of permissions, credentials, and secrets.

In this report, we propose a maturity model to be used by enterprise teams to gauge how well they are handling this important administrative function. The goal is not to establish a metric for comparison in the context of vendor selection or competitive review, but rather as a means for an organization to challenge itself to improve. Such emphasis is important, because different companies will have different context, so comparison to oneself is the best approach.

## CHALLENGE OF MANAGING PERMISSIONS

The challenge of managing and securing permissions is well-known, but too many organizations still have not created an environment where this is not a serious vulnerability. One reason is that entitlements, access, permissions, and the like create a complex ecosystem of data, relationships, operations, and interactions. For large organizations, this requires automated support just to keep up.

As a result, significant deficiencies often emerge in the following broad areas:

- *Provisioning* – Threats emerge in sloppy provisioning environments for obvious reasons. This stage of the permissions lifecycle is where baseline configurations and settings are established. Over-permissioned infrastructure assets can be vulnerable to attacks – again, for obvious reasons.
- *Administration* – The day-to-day administration of permissions and credentials is easier said than done, especially when an organization has non-trivial complexity. In general, automation should be the primary goal to help reduce the potential for human errors or insider attacks.
- *Protection* – The securing of permissions is often missed, which is ironic because the purpose of entitlements management is, in fact, security. Nevertheless, security tools, procedures, and policies must be in place to avoid weak configurations and bad permissions management.
- *Usage* – The day-to-day use of organizational resources (e.g., applications, systems, networks) relies heavily on a clean permissions environment. In addition to introducing security weaknesses, sloppy handling of permissions also creates user friction and reduces their ability to get their jobs done. It also attributes to the fears of business disruption in the event a permission needs to be changed.
- *Retirement* – The final step in the permissions management and protection lifecycle includes proper retirement. When this is not done properly, hackers can exploit orphaned accounts and entitlements to gain unauthorized access to valuable assets and resources. Also, unnecessary legacy access causes confusion and unnecessary clutter, making it harder to spot the biggest risks.

The maturity model introduced in the next section describes three levels of capability for these broad areas of permissions management and security. The goal is to create a means for an organization to improve its own operation, as well as to help direct mature behaviors in this area from its suppliers, partners, and other third-party (and fourth party) business organizations.

## MATURITY MODEL

The maturity model introduced here includes three levels of operation, which we refer to as *baseline*, *intermediate*, and *advanced*. Each successive level in the model from baseline to advanced includes improved handling of permissions and entitlements and deploys more preventative controls to ensure that violations and excess provisioning will not occur. The levels are described below.

## **Level 1: Baseline**

Baseline maturity for entitlements management is the lowest level of operation. It might be an acceptable choice for smaller companies, but it will not be an effective approach for organizations with non-trivial infrastructure, large employee bases, and use of many different systems and applications. Regulated industry should not even consider this level as an option. Heavy multi-cloud use, for example, is an indicator that this baseline maturity level will not be sufficient.

### *Entitlements – Identified*

Entitlements are identified for access to data, applications, and systems. Controls might not be clearly defined, and the identification might not be integrated into a managed inventory, but at least some entitlements identification process can be found for ad-hoc support needs.

### *Least Privilege – Policy Defined*

The organization defines its support for least privilege enforcement in all applicable areas of identity and access management. Such support might not be strongly enforced with strict controls, but the policy definition can be found.

### *Entitlement-Related Data – Identified*

Metadata related to entitlements including the permissions owner, granting entity, corresponding access rights, and so on – can be identified. The identification might not include all relevant metadata, but at least some meaningful effort is being applied.

### *Administration – Manual, Ad Hoc*

Administration and maintenance of entitlements is done using mostly manual processes that are driven by ad hoc events, rather than some well-defined set of scheduled and managed tasks using automated support.

### *Visibility – Manual, Ad Hoc*

Visibility into the management of entitlements including any anomalies or unexpected permissions allocation is obtained manually and on an ad hoc basis without the use of an automated system to provide comprehensive views.

### *Analysis – Manual, Ad Hoc*

Analysis of entitlements posture including any reviews of over-permissioned systems or improperly allocated entitlements is done manually without the use of tools that can identify deviations from profiles or learned models.

### *Data – Ad Hoc Support*

The data (and metadata) supporting the management of entitlements is obtained mostly manually from users without the use of connectors or API-based transfer of ad hoc information from relevant automated systems, directories, and applications.

### *Remediation – Manual*

Remediating any issues that arise with entitlements management is done manually based on available information about the problem without use of automated response or workflow platform or tools.

## **Level 2: Intermediate**

The intermediate level of maturity is likely to match up with the most common approach used by larger organizations today. It is characterized by a transitional, hybrid use of manual processes and



automated tools. Inclusive of the lower baseline approach, this maturity level serves as an excellent gateway toward the highest level of maturity which maximizes the use of automation and platform leverage.

#### *Entitlements – Identified and Managed*

Entitlements are clearly identified for access to data, applications, and systems and integrated into a managed inventory. An entitlements management process can be identified that ensures on-going tracking, review, and update of permissions and other data.

#### *Least Privilege – Reviewed and Assessed*

The organization defines its support for least privilege enforcement in all applicable areas of identity and access management. Such support is enforced with controls, and the least privilege goal can be found in corporate policy documentation.

#### *Entitlement-Related Data – Collected and Improved*

Metadata related to entitlements including the permissions owner, granting entity, corresponding access rights, and so on – can be identified. The collection process includes all relevant metadata, and process improvements exist to improve data quality.

#### *Administration – Tool-Assisted*

Administration and maintenance of entitlements is done using manual processes that are assisted by automated tools, into a reasonably well-defined set of scheduled and managed tasks using the automated support.

#### *Visibility – Tracking Tool-Assisted*

Visibility into the management of entitlements including any anomalies or unexpected permissions allocation is mostly manual but does use of automated tools to improve the overall process and increase the scope of visibility.

#### *Analysis – Tool-Assisted*

Analysis of entitlements posture including any reviews of over-permissioned systems or improperly allocated entitlements is mostly manually but does use automated tools to help identify deviations from profiles or learned models.

#### *Data – Structured*

The data (and metadata) supporting the management of entitlements is obtained mostly manually from users with some assistance of connectors or API-based transfer of structured information from relevant automated systems, directories, and applications.

#### *Remediation – Coordinated With Remediation Tools and Processes*

Remediating any issues that arise with entitlements management is manually based on available information about the problem with coordinated assistance of automated response or workflow platforms and tools.

### **Level 3: Advanced**

The advanced maturity level for entitlements management includes continuous support of automated platforms to validate and enforce security. It includes use of the most advanced technology available, and it allows teams to track changes, use embedded workflows, and consolidate data from various sources. It should be the target level for any large company with a complex deployment of entitlements.

#### *Entitlements – Continuously Validated and Enforced*

Entitlements are clearly identified for access to data, applications, and systems and integrated into a managed inventory. An entitlements management process can be identified that ensures on-going tracking, review, and update with continuous validation and enforcement.

#### *Least Privilege – Continuous Enforcement of Privilege Policy*

The organization defines its support for least privilege enforcement in all applicable areas of identity and access management. Such support is continuously enforced with automated controls, and the least privilege goal can be found in corporate policy documentation. Regular certification of access is enforced, and any new areas of excessive access are immediately resolved.

#### *Entitlement-Related Data – Consolidated From Different Sources*

All relevant metadata related to entitlements including the permissions owner, granting entity, corresponding access rights, and so on – can be identified. The collection process includes process improvements and consolidates data from all sources to improve data quality. There is a single source of truth with the necessary integration points into key systems and downstream processes.

#### *Administration – Embedded Workflow Using an Automated Platform*

Administration and maintenance of entitlements is done using an automated platform that includes embedded workflow, as part of a well-defined set of scheduled and managed tasks using automated support.

#### *Visibility – Broad Continuous Tracking Across Enterprise*

Visibility into the management of entitlements including any anomalies or unexpected permissions allocation is broad and continuous with use of automated tools to improve the overall process, tracking, and the scope of visibility. Stock and flow reporting is available to demonstrate reduction of risk in identified areas that require remediation, alongside the tracking mechanisms to ensure new risk is not being created in parallel.

#### *Analysis – Includes Correlation of Accounts, Servers and Applications*

Analysis of entitlements posture including any reviews of over-permissioned systems or improperly allocated entitlements uses an automated platform to help identify deviations from profiles or learned models with correlation of accounts, servers, and applications. The production of key KRIs should be automated and refreshed on a regular basis.

#### *Data – Support for Structured and Unstructured*

The data (and metadata) supporting the management of entitlements is obtained from users with the use of connectors and API-based transfer of structured and unstructured information from relevant automated systems, directories, and applications.

#### *Remediation – Integrated Platform-Based Support for Pruning, Elimination and Removals*

Remediating any issues that arise with entitlements management is automated and platform-integrated based on available information about the problem with assistance of automated response or workflow platforms and tools to prune, eliminate, and remove anomalies.

#### *Controls and Measures – Automated and Continuous*

The controls in place to provision, administer and monitor access are known and catalogued. Regular assessment of these controls is undertaken to determine their design effectiveness and automated metrics and KRIs (key risk indicators) are produced to measure their operational effectiveness. Continuous assessment and improvement of access controls is undertaken.

	<b>Level 1: Basic</b>	<b>Level 2: Intermediate</b>	<b>Level 3: Advanced</b>
<b>Entitlements</b>	Identified	Identified and Managed	Continuously Validated and Enforced
<b>Least Privilege</b>	Policy Defined	Reviews and Assesed	Continuous Enforcment of Privilege Policy
<b>Entitlement-Related Data</b>	Identified	Collected and Improved	Consolidated from Different Sources
<b>Administration</b>	Manual, Ad Hoc	Tool Assisted	Embedded Workflow on Automated Platform
<b>Visibility</b>	Manual, Ad Hoc	Tracking Tool Assisted	Continuous Tracking Across Enterprise
<b>Analysis</b>	Manual, Ad Hoc	Tool Assisted	Correlation of Accounts, Serves, and Applications
<b>Data</b>	Ad Hoc Support	Structured	Support for Structured and Unstructured
<b>Remediation</b>	Manual	Coordinated with Tools and Processes	Integrated Platform Support
<b>Controls &amp; Measures</b>	<b>Manual / Ad Hoc</b>	<b>Partially Automated</b>	<b>Automated &amp; Continuous</b>

Figure 1. Maturity Model for Entitlements Management

## ACTION PLAN

Enterprise teams who must manage entitlements, permissions, and related identity and access management credentials, data, and supporting metadata should first establish their own level of maturity in the model proposed here. This assessment can be self-performed or could be assisted with an external consultant familiar with the specifics of how entitlements are performed within the enterprise.

Based on the maturity assessment, the organization should use a local understanding of the relevant cyber threats, available budget, and identity and access management objectives can serve as the basis for identifying a target maturity level. The goal should be to continuously expand coverage of vetted processes as well. Identification of a suitable commercial platform is likely to be an important aspect of any initiative focused on increasing the maturity level of the organization for entitlements management toward improved cyber hygiene.

# EVIDENCING CYBER RESILIENCE VIA SIMULATIONS AND SCENARIOS: AN OVERVIEW OF IMMERSIVE LABS

EDWARD AMOROSO

---

A novel approach is introduced by Immersive Labs for measuring and improving cyber readiness skills across the enterprise. This goal is accomplished via tailored simulations and scenario exercises designed for both the security team and the full organization.

## INTRODUCTION

The need for cybersecurity training and skills development is well-established in the community. Tailored range training for security operations center (SOC) teams, for example, has been an important new aspect of enterprise protection and has helped many expert teams to improve their ability to work together under pressure. War game exercises have also been a common tool to help teams develop better skills for cyber readiness.

Similarly, individuals have many personalized options to learn cybersecurity. Universities and professional training organizations, for example, offer courses, lectures, hands-on labs and other forums for anyone needing to refine their skills or just wanting to make better decisions about security issues such as phishing attacks. TAG Cyber has covered this sector and has identified many excellent training platform options.

Three challenges that remain, however, with respect to enterprise cyber readiness include measurement and coverage. Regarding measurement, we believe that no good method has existed to date for analyzing a cyber readiness posture in the context of a generally accepted metric. Regarding coverage, we mean that most training to date has only included isolated teams or groups, rather than the entire organization.<sup>1</sup>

A third challenge involves the problem of being able to evolve human capabilities at a rapid pace. For many years, the industry has focused on static certifications that fill a resume, versus having some means for emphasizing and enhancing the skills required to deal with live resilience issues as they emerge. Skills must be updated at the same pace as the risks to the organization.

The Immersive Labs<sup>2</sup> solution focuses on all three areas—and hence the deeper investigation here by the TAG Cyber team. This included multiple reviews with the Immersive Labs team, as well as brainstorming sessions with enterprise teams trying to improve their cyber readiness.<sup>3</sup> This report outlines the various advantages discovered in the Immersive Labs approach, along with recommendations on how an enterprise can make best use of the solution.

## MEASURING CYBERSECURITY MATURITY

Some prior effort has been directed toward measuring the degree to which a security team is ready for future cyberincidents. Maturity models, in particular, can be used to baseline the types of capabilities and functions that an organization should include for cyberprotection. The CMMC (Cybersecurity Maturity Model Certification) program of the U.S. Department of Defense, for example, includes a range of levels designed to differentiate organizational readiness.

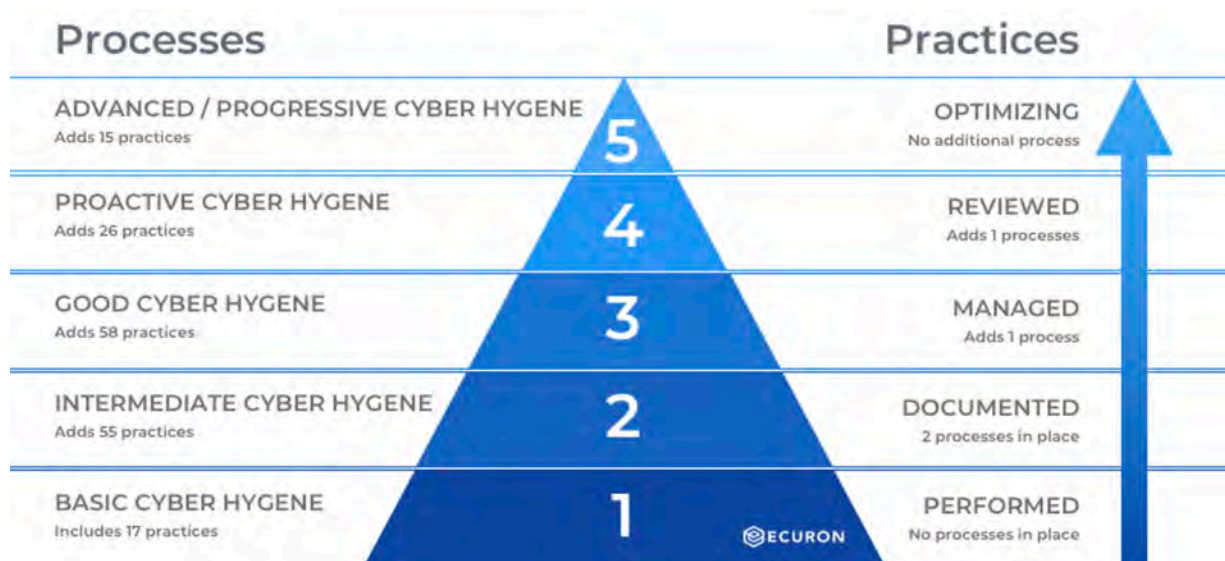


Figure 1. The Five Levels of the U.S. DoD CMMC Model

The problem with CMMC and similar maturity levels is that they tend to focus on processes and their relationship to program objectives. They also tend to ignore one of the most salient aspects of readiness: the skill level of the groups involved in protection. The degree to which they can interpret data, work together toward a common goal, and coordinate on a reasonable response is not easily measured in a maturity model.

## MEASURING CYBERSECURITY SKILLS DEVELOPMENT

To develop metrics for cybersecurity skills training, a different approach is required—one that includes the use of simulations, exercises and other live engagements for individuals, groups, teams and

even the entire organization. This approach is closely related to security education and training, but is differentiated by its focus on metrics and its use of tailored engagements versus more traditional coursework learning.

The way that such engagements work involves several phases of tailored work by experts in cybersecurity skills training (such as Immersive Labs—see below), as well as the organization's efforts to measure and improve its skills. These phases begin with preparation-type activities, continue through execution of the engagements, employ metrics-based assessments, and then loop around continuously. The specific phases are as follows:

- *Step 1: Identification of Business Mission Objectives*—Security readiness must be focused and measured according to the mission of the organization, which will vary from one company or sector to another.
- *Step 2: Selection of Individuals, Groups and Teams*—The scope of any security readiness training or improvement initiative must include clarity around which individuals and teams would be involved.
- *Step 3: Tailored Design of Security Skills Engagements*—Great security readiness initiatives avoid use of one-size-fits-all scenarios to test and measure effectiveness in dealing with attack campaigns.
- *Step 4: Collection of Data and Metrics*—The data that can be collected during emulated situations or simulated lab tests must be associated with clear metrics, goals and improvements objectives.
- *Step 5: Management Learning and Action*—The best organizations understand that skills improvement can come only through an ongoing program of continuous management, learning and actions focused on addressing weaknesses.

While the steps shown above are generalized, and will vary in different groups, they illustrate the common discipline required to drive skills assessment, improvement and monitoring. In the next section, we introduce and explain the approach taken by commercial cybersecurity company Immersive Labs to implement many of the concepts addressed above to help organizations optimize their readiness for cyberincidents and campaigns.

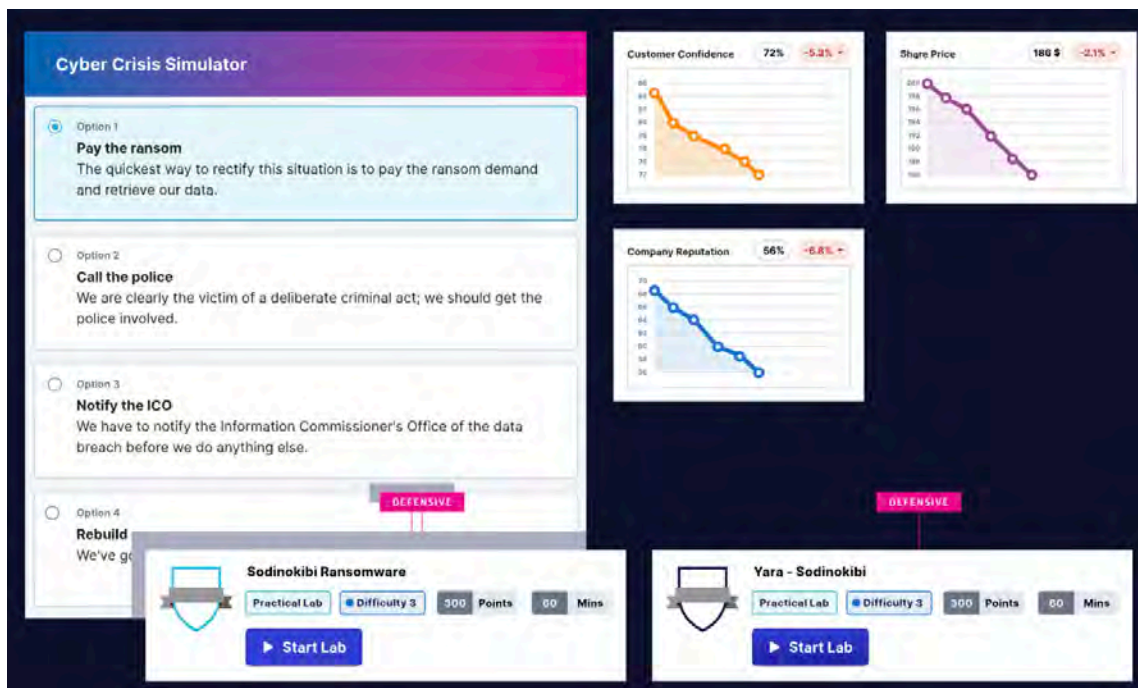
## UNDERSTANDING THE IMMERSIVE LABS APPROACH

Founded in 2017 and headquartered in the United States and the United Kingdom, Immersive Labs supports a platform and associated set of capabilities that optimize the ability of a workforce to deal with present and future cyberthreats. As a component of new cyber workforce optimization (CWO) initiatives, the Immersive Labs solution has emerged as a key aspect of enterprise protection.

The Immersive Labs solution is based on three pillars of CWO, which are described by the company using three mnemonic phrases: Exercise, Evidence and Equip. These three focus areas help to organize and demonstrate how an enterprise can work with Immersive Labs to optimize its own ability to deal with advancing cyberthreats and to have clear posture metrics on how this defensive posture is improving.

### Exercising to Test Resilience

The process of exercising an organization for cyber readiness involves creation of realistic simulated scenarios. These are best developed in the context of threat intelligence and information about the most likely types of attacks that a company is likely to experience from an adversary. The idea is to highlight, via the exercises, where teams might have vulnerabilities or challenges in responding.



**Figure 2. Sample Exercise Reporting Screen—Crisis Simulator**

### Collecting Evidence to Prove Cybercapabilities

The process of collecting evidence is driven by the MITRE ATT&CK framework, which offers an industry-accepted baseline of attack tactics. Obviously, metrics that apply to the larger organization will generalize beyond the more specific ATT&CK techniques, but in all cases, evidence collection must be done in the context of a clear baseline and should include real-time tracking capability to help visualize posture.

### Equipping an Enterprise With Cybercapabilities

The process of equipping an organization with resilience capabilities should be aligned with the results of exercises and the evidence collected about current posture. The goal is to support strategic cyber risk decision-making, and to ensure that selected security safeguards and controls are relevant to the existing risks, and timely with respect to the most recent threats being experienced across the global environment.

The Immersive Labs platform includes an offensive lab that offers hundreds of cybersecurity skill experiences that can be used in a test and simulation context to exercise readiness. This includes establishing objectives for roles such as penetration tester, and exercises in areas such as web attacks and exploits. Capture the flag (CTF) exercises are included in the suite as well.

The platform also includes a corresponding defensive lab that supports hundreds of protection experiences that can be used to drive readiness for security analysts, threat hunters, incident responders and other enterprise professionals. Hands-on labs are provided for roles such as SOC analyst, and exercises are included that focus on security methods, such as reverse engineering and threat hunting.

The platform complements the offensive and defensive labs with skills guidance and testing for secure coding, using popular languages and frameworks; candidate screening, by exposing the individual

to live exercise conditions to measure their security and coordination skills; awareness focus, using gaming to improve engagement and learning for the entire company; and crisis simulations, to drive readiness for the executives and managers of the organization.

All of these capabilities drive a broad benefit to executives, managers and practitioners by making them more able to deal with resilience challenges as they emerge. Crisis simulation, in particular, helps senior executive teams prepare for incidents that can impact the critical mission of the business.

## **PROPOSED ENTERPRISE CYBER READINESS ACTION PLAN**

Enterprise management teams and their security experts who seek to measure, improve and maintain readiness skills for cybersecurity are advised to engage an action plan immediately. While the specifics between organizations will certainly vary, the major elements of such an action plan for cybersecurity skills optimization and protection readiness for cyber risk would include the following tasks:

### *Task 1: Inventory of Existing Learning and Skills Development Activities*

To successfully deploy a learning and skills development program, it is essential to start with an inventory of existing similar programs within the organization. A cooperative approach is always best, and companies with mature learning initiatives would be wise to find ways to integrate cybersecurity skills learning with other programs.

### *Task 2: Development of Key Performance Indicators and Readiness Goals*

Organizations are advised to spend time identifying the performance objectives and goals for the cybersecurity readiness program. This can be codified as key performance indicators (KPIs), or as more general goals to be expressed in the context of expected outcomes for different types and categories of incidents.

### *Task 3: Engagement With a Commercial Solution Partner*

The TAG Cyber team recommends engagement with a commercial solution partner such as Immersive Labs to ensure an optimal cybersecurity skills readiness program. Keeping up with changing threats and evolving tactics requires the full-time attention of an expert team, and few organizations could possibly fund and support such an initiative.





ANALYST REPORT

# PROTECTING THE EVERYWHERE WORKPLACE: AN OVERVIEW OF IVANTI CYBERSECURITY

EDWARD AMOROSO

---

Modern enterprise users have expanded their computing usage and remote access to an everywhere workplace. Cybersecurity solutions must therefore include the scale and reach of IT service management systems. The Ivanti Neurons platform<sup>1</sup> exemplifies this coverage for secure access, zero trust and intelligence.

## INTRODUCTION

The trend toward an everywhere workplace had gained momentum long before workers began staying home because of pandemic concerns. The obvious cost and productivity advantages of more flexible workstyles became so evident in recent years that companies around the world began to fundamentally reinvent how their employees and support staff would coordinate and cooperate around businesses processes.

As one would expect, however, the cybersecurity requirements that come with a distributed remote workforce are different from the legacy controls that evolved around the traditional enterprise perimeter. As part of this change, zero trust security has become the new design paradigm for any hybrid enterprise where users depend on endpoints to access cloud or SaaS-hosted apps over public broadband or wireless services.

In this report, we explain how an integrated cybersecurity platform is best to serve such work-from-everywhere enterprise teams—and how underlying IT service management forms an excellent base on which to build strong controls. The commercial Ivanti Neurons platform is used to illustrate this desirable integration for secure access, zero trust security and patch intelligence solutions.

## WHAT ARE THE THREATS TO WORK-FROM-EVERYWHERE?

Traditional IT support was greatly simplified by the proximity and commonality of uniform devices, operating systems and applications—all protected by a firewall-oriented perimeter that separated untrusted external entities from trusted internal users. IT service management (ITSM) platforms were originally created to address this type of computing environment, and they tended to include security support for antivirus and scan management.

More recently, however, enterprise computing has expanded to public cloud services, SaaS infrastructure, mobile applications and even social media. In addition, the end user has exited the cubicle, instead using a laptop or mobile device to accomplish work tasks outside the normal business environment. Cloud and SaaS apps are particularly well-suited to this architectural shift outside the perimeter.

The security advantage, obviously, with this shift to work-from-everywhere is that security dependence on the enterprise perimeter is greatly reduced. This is an improvement over the existing challenges of trying to police an increasingly leaky perimeter, not to mention the problem of compromised insiders. To leverage this advantage, however, security teams must contend with the new threats associated with this shift:

- Expanded Cloud Security Dependence—By shifting support from the enterprise IT team to third-party service vendors, including especially the major cloud providers, security teams inherit the risk that these groups might be compromised. The good news is that the corresponding risks of internal management are reduced, but some changes in how threats are assessed and mitigated in the cloud are required.
- Expanded Visible Attack Surface—The traditional attack surface for most enterprise teams has been perimeter-focused. This approach simplifies scanning and related tasks aimed at providing visibility into any exploitable weaknesses. But expansion to cloud and SaaS will obviously increase the attack surface, and might also prompt changes in how an attack surface is identified and reduced.
- Reduce Physical Protection—The physical protections that were central to legacy data center security become less relevant when applications move to public infrastructure. This also extends to physical controls that change when user devices such as laptops and PCs are stored, accessed and used outside the enterprise. Work-from-home carries the obligation to train employees on how to protect their physical devices.
- 

These new threats are balanced by the advantages of work-from-everywhere initiatives. Such advantages include not only productivity and flexibility improvements, but also (as suggested above) actual cybersecurity gains. This is particularly true for any enterprise that struggles to hire the staff they need and to gain a budget sufficient to buy best-in-class security tools. Shifting to public cloud and SaaS connects customers with great staff and the best tools.



Figure 1. New Cyberthreats Emerging From Work-From-Everywhere

## ITSM AS A FOUNDATION FOR CYBERSECURITY

One foundational component that helps to leverage the benefits of work-from-everywhere while also helping to address the various new risks is ITSM. Recognized by both IT operations and cybersecurity teams as vital to the proper operation of all endpoints, systems, networks and applications, ITSM tools and platforms provide an underlying base for computing management, coordination and support.

Because so many enterprise teams are organized with separate IT operations and cybersecurity staff (usually resident in different organizations), ITSM infrastructure is often neglected by security teams in the establishment of their protection architecture and planning. This is unfortunate, because ITSM offers precisely the type of visibility, reach and control necessary to handle an expanded attack surface.

An implication is that ITSM should play a role in the creation of modern security protection schemes for the transition to work-from-everywhere. This should include the use of ITSM for the following security tasks:

- *Visibility*—One of the great advantages of a modern ITSM platform is the visibility afforded to digital assets. This helps to optimize inventory, which is a difficult task in a distributed work-from-everywhere environment. As such, the active and passive scanning capabilities that come with ITSM are essential to managing cyber risk in an evolving hybrid IT environment.
- *Support*—The IT support capabilities inherent in an ITSM platform are also essential to dealing with the day-to-day needs of a distributed workforce. The opportunity for workers to locally share best practices in security is difficult to duplicate properly in a virtualized work-from-everywhere setting. ITSM can be used to bridge this security support gap.
- *Mitigation*—The task of either preventing or responding to cyberincidents becomes more complicated when resources are distributed outside the traditional enterprise. As such, ITSM can enable fast mitigation, such as patching, updates or changes in policy rules. This must be implemented with sufficient reach to the variety of end-user configurations that come with work-from-everywhere approaches.

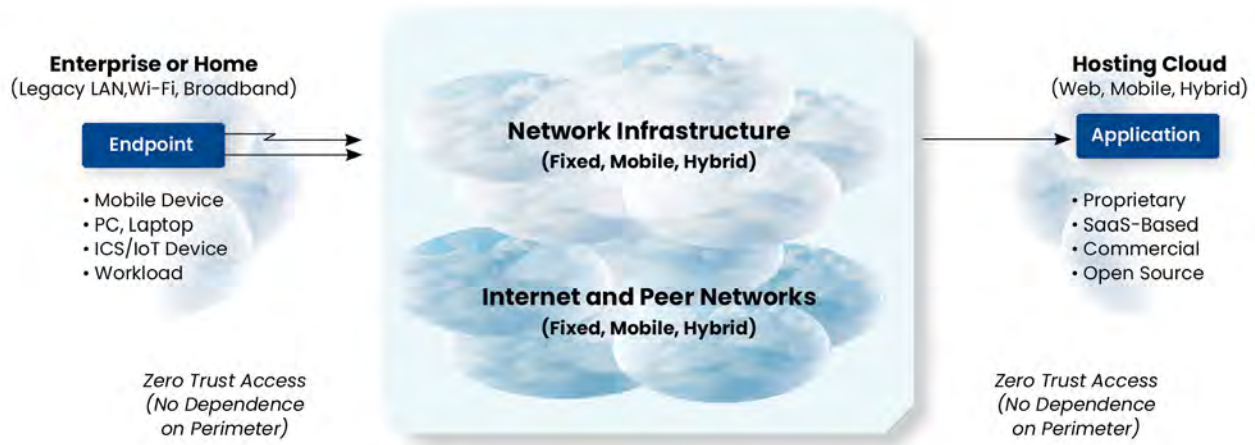
This central role of ITSM for cybersecurity in modern hybrid IT environments is good news for most organizations, because commercial support platforms are often in place. This allows for leveraging existing functions to support cybersecurity initiatives. In the next section, we outline the industry-leading Ivanti Neurons platform, which combines best-in-class ITSM functions with modern cybersecurity capabilities.

## OVERVIEW OF IVANTI CYBERSECURITY SOLUTIONS

Headquartered in the U.S, with offices in 23 countries, Ivanti supports IT service management for companies around the world and in every sector. Cybersecurity is a major aspect of this commercial offering, and it has grown through a combination of organic extension and the acquisition of best-in-class cybersecurity vendors. Ivanti Neurons serves as the automation platform base for its unified endpoint, zero trust and enterprise service management solutions.

Key recent cybersecurity acquisitions for Ivanti include MobileIron in 2020, Pulse Secure in 2020 and RiskSense in 2021. Each of these additions to the portfolio provides enhanced capability to protect work-from-everywhere initiatives, and each supports the concept of zero trust security. Security practitioners now agree that zero trust, which emerges in the context of a de-perimeterized network, is well-suited to a distributed workforce.

Ivanti cybersecurity solutions are organized around the goal of securing work-from-everywhere initiatives. This is done via zero trust security through portfolio components that support the foundational aspects of ITSM for cybersecurity referenced throughout this report. This includes visibility, support and mitigation for protection of enterprise IT infrastructure against cyber risks, especially with extension to distributed work. Specific components are listed below.



**Figure 2. Zero Trust for Work-From-Everywhere**

### *Ivanti Neurons for Secure Access*

This involves modernization of VPN deployments through centralized zero trust platform support from Ivanti Connect Secure and Ivanti Neurons for zero trust access management. Implemented as a cloud-accessible platform, the primary features include SaaS support for hybrid IT, integration with existing VPNs and support for a software-defined perimeter. These capabilities are essential to modern work-from-everywhere initiatives.

### *Endpoint Security for Endpoint Manager*

This is composed of a single integrated security solution for all devices and critical data on an enterprise network, with support for distributed workforce management. The types of security capabilities included are monitoring, evaluation, remediation, verification and mitigation of security issues. This includes support for compliance and patching, which remain central to cyber risk reduction for large deployments of endpoints.

### *Mobile Threat Defense*

This involves defense and remediation of threats to mobile devices, including protection against mobile phishing. Such capability is founded on the industry-leading MobileIron platform and is built into the endpoint management capability to optimize administration and usage. The solution also enforces policies to prevent users from disabling the mobile security, perhaps by attempting to remove it from the device.

### *Policy Secure (NAC)*

This capability offers visibility and network access control for all local and remote endpoints. This is essential for work-from-everywhere, because it supports enforcement of security compliance for the PCs, laptops and other devices being used to access corporate resources in the cloud, SaaS or legacy environment. Acquisition of the Pulse Secure platform enables this feature in the Ivanti portfolio.

### *Zero Sign-On*

This feature is designed to remove dependence on password usage for access to cloud, SaaS and data center-hosted applications and systems. Zero sign-on supports multicloud use by ensuring that business data cannot be stored on unsecure data. The solution is designed to support both managed and unmanaged endpoints and becomes the basis for advanced authentication without the encumbrance of passwords.

# RISK-BASED MANAGEMENT OF THIRD-PARTY CYBERSECURITY EXPOSURES: AN OVERVIEW OF PREVALENT

EDWARD AMOROSO

---

In this paper, we introduce a foundational risk model, and map high-priority third-party cyber risks found in the typical modern enterprise to that model. The resulting framework provides effective guidance for enterprise teams selecting third-party cyber risk platform solutions. The Prevalent platform aligns well with the elements of this third-party risk framework.

## INTRODUCTION

Ask any modern chief information security officer (CISO) which cyberthreats are the most concerning to their business, and most will point to third-party supplier risk as their primary issue. The annual Verizon Data Breach Investigations Report (DBIR), for example, regularly references challenges in dealing with external suppliers and partners as the weakest link in every enterprise cybersecurity program.<sup>1</sup>

The conundrum in dealing with third parties is that while businesses select and trust these entities to carry out important aspects of the organizational mission, they cannot always confirm that security is being attended to properly. Asking, or even demanding, that third-party suppliers focus on security is a reasonable first step, but business requirements that more dependable controls be put in place.

In this report, we introduce a simple foundational risk model that can be used to establish an effective cybersecurity program to address third-party threats. The goal of any third-party risk model and the program is to ensure continued value from suppliers while also reducing risk to maintain security and compliance. We use the Prevalent Third-Party Risk Management (TPRM) Platform to exemplify these concepts in a practical enterprise setting.

## THIRD-PARTY RISK MANAGEMENT CHALLENGES

The evolution of the modern information technology (IT) infrastructure continues to fuel the rapid increase in the use of third-party services. Most managers have decided that it is faster and cheaper to use an externally supported platform or service than to build the capability in-house. This creates significant risk challenges for enterprise teams. Below we explain the more prominent areas that require security and compliance attention.

### *Third-Party Cyber Risk: Software*

Managing software risk for third-party partners and suppliers can be a significant challenge. There are countless practical examples of third parties that rely on highly vulnerable open source software libraries, or whose services and solutions will only run with outdated third-party components, such as Java. These software decisions by third parties create significant risk problems for CISOs.

For example, one of the widest-reaching third-party breaches in history resulted from malware being delivered as part of a SolarWinds Orion software update.<sup>2</sup> In this case, any enterprise that was diligently following industry-standard patching processes inadvertently installed a malware-laden software package that provided malicious actors with full access to enterprise infrastructure.

### *Third-Party Cyber Risk: Compliance*

Most security and risk teams have accepted that the best way to ensure that a third party has adequate security and risk mitigation controls is to measure them against standards such as NIST CSF, ISO2700x, Cloud Security Alliance CAIQ or SOC 2. These frameworks are useful because they ensure a common approach across multiple environments, including the diversity that emerges when multiple suppliers and vendors are being supported. However, organizations struggle with complexity in compiling and reporting on security controls across a large supplier ecosystem.

Compliance Framework	Framework Sponsor	Brief Framework Description
NIST CSF	U.S. National Institute of Standards and Technology	The NIST Cybersecurity Framework (CSF) integrates best practices for identifying, protecting, detecting, responding and recovering from cyberthreats to enterprise teams.
ISO 2700x	International Standards Organization	ISO created the 2700x series of standards to guide the assessment and treatment of information security risks and the associated controls embedded in IT security management systems.
CSA CAIQ	Cloud Security Alliance	The Consensus Assessment Initiative Questionnaire (v3.1) offers straightforward guidance on documenting the controls in PaaS, IaaS and SaaS infrastructure.
SOC2	American Institute of CPAs	SOC 2 is an auditing standard and procedure designed to ensure that service providers are managing and protecting customer data sufficiently.

**Figure 1. Common Compliance Standards to Address Cyber Risk**

### *Third-Party Cyber Risk: Fraud*

Another challenge that many enterprises face is the tracking and monitoring of vendors from an antifraud and compliance perspective. In recent years, the federal government has stepped up

its enforcement of the Foreign Corrupt Practices Act (FCPA), with significant fines being levied on organizations that turn a blind eye to bribery performed by a third party on their behalf.

This is a particularly tough challenge for cybersecurity teams that have excellent technical or operational backgrounds but perhaps little experience in dealing with such illegal action. In such cases, a partnership between the security teams and corporate security, antifraud experts, legal support and even finance groups can be useful to address the risk.

#### *Third-Party Cyber Risk: Responsibility*

The Securities and Exchange Commission (SEC) has repeatedly stated that all U.S. companies must now accept full responsibility for third-party agents acting on their behalf. Understanding the compliance and ethics risks associated with so-called red-flagged agents has now emerged as a critical risk mitigation obligation for most enterprise security risk and compliance departments.

Accepting such responsibility also introduces the issue of the transitive chain that emerges when third parties have their own third parties, thus creating a fourth- and even fifth-party risk. Extending controls this far out from local security controls is arguably beyond the current state of the practice, but it is quickly becoming a significant enough issue to warrant improved protection.

#### *Third-Party Cyber Risk: International*

In a similar vein, tracking sanctioned vendors, especially in the current political environment, can be time-consuming. Given the Encryption and Export Arms Regulations (EAR), the International Traffic in Arms Regulations (ITAR) and the frequently changing U.S. Treasury's Office of Foreign Assets Control (OFAC) list, modern enterprises must understand and adapt to the risk associated with third parties flagged by the U.S. government as potential bad actors.

For international organizations, the multitude of privacy regulations and data sharing agreements forces specific monitoring of PII information, why it's being shared, with whom it's being shared, and what happens to the data during and after the contract's lifespan. Vendor adherence to the European Union (EU) General Data Protection Regulation (GDPR); the California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA); and the New York Department of Financial Services (NYDFS) regulations must be managed and monitored from contract inception through termination.

#### *Third-Party Cyber Risk: Complexity*

An additional challenge for enterprise teams trying to manage third parties is the complexity of the internal processes. The process is familiar: IT defines a need; procurement identifies the potential vendors; RFPs are issued; downselection occurs; and winners are chosen. Compliance is then asked for an OFAC review; legal is engaged to review the terms (typically, striking parts of the contract); SLAs are defined; KPI penalties are set; and the document is executed.

Usually little consideration is included as to how the legally binding metrics will be collected and reported. The entire process is marred by deeply embedded processes, ambiguous language and competing business drivers. Risk frameworks can assist with this challenge. In the next section we will show how the most common equation for risk can be mapped to the challenges of third-party security.



## FOUNDATIONAL RISK MODEL FOR THIRD-PARTY SECURITY

Every cyber risk model must include the likelihood (or probability) of malicious actions targeting valued assets, as well as the associated consequences of such threats. This produces the canonical equation of risk being the product of likelihood and impact (often designated informally as  $R = P * C$ ). When consequences are expressed in terms of financial loss, the risk model is more easily integrated into most environments. The FAIR model, for example, includes such emphasis.

As such, it is reasonable to start with this foundational model for how third-party risk might be addressed. This is done by mapping the components of the model—namely, probability and consequences—into the framework of third-party business interactions with suppliers, partners and other external business entities. The result is a useful means for measuring the effects of third-party security decisions on overall enterprise risk.

The factors best applied to such mapping are the specific elements cited above, including third-party issues for software, compliance, fraud, risk acceptance, international and complexity. Each of these aspects of the third-party risk equation introduces a deeper view into the probability and consequences for a given enterprise using third-party partners or suppliers to accomplish their mission. The mapping is shown in Figure 2.

Third-Party Cyber Risk	Probability of Occurrence	Consequences of Occurrence
<b>Software</b>	Depends on the degree to which the third-party support is dependent on or involves provision of software.	Based on types of assets that are directly or indirectly affected by third-party software cyber risks.
<b>Compliance</b>	Depends on which compliance frameworks are relevant to the parent organization using third-party support.	Based on the legal, regulatory or policy implications of third-party noncompliance with key requirements.
<b>Fraud</b>	Depends on the organizational mission, and whether fraud and abuse are applicable threat use cases.	Based on the financial gain an intruder might obtain as a result of third-party fraudulent action or abuse.
<b>Responsibility</b>	Depends on contractual terms, but will generally involve the organization being responsible for third-party action.	Based on the agreed-upon terms of the third-party support, and whether it is involved in key aspects of the mission.
<b>International</b>	Depends on the degree to which the relevant third-party support is being provided from international locations.	Based on international laws, regulations or policy, and whether the third party can produce adverse effects.
<b>Complexity</b>	Depends on the specific type of third-party support, and whether complex functions and processes are present.	Based on the nature of the third party support, and how risks might occur from overly complicated functions.

Figure 2. Mapping Foundational Risk Model to Third-Party Security

To properly perform this desired foundational mapping, it helps to work with a commercial vendor that not only understands the specifics of third-party risk, but also implements a platform that can simplify the process of identifying, managing and reporting the actual risks that exist for the organization from its portfolio of third-party suppliers, partners and other entities.

## COMMERCIAL SOLUTION REQUIREMENTS

Cybersecurity companies now offer commercially available third-party risk management solutions that effectively address the foundational issues described above, using single consolidated platforms. Below we discuss several of the more prominent features in a desired platform and map each feature directly to the corresponding component of our third-party risk model to demonstrate coverage.<sup>3</sup>

### *Vendor Sourcing and Selection*

A commercial third-party risk management platform must address the procurement lifecycle during vendor selection and contracting. It should manage the lifecycle of a contract and send automated assessment inquiries to ensure alignment with corporate policies prior to final vendor selection. Such broad capability lines up well with each of the probability and consequences issues included in the foundational risk model described above.

### *Centralized Vendor Onboarding*

By having a single source of truth, a commercial third-party risk management platform provides all interested parties with a single source for all vendor records. Compliance can validate requirements, enforce legal constraints and ensure that the contract is managed correctly. Also, the information security and risk teams can review vendor-related technology risks by mapping interrelationships in the platform.

### *Inherent Risk Scoring*

Compliance teams are being required to review vendors for FCPA, OFAC and other violations, as well as to understand the inherent security risks that new vendors bring—prior to contract execution. A third-party risk management platform should include custom, business or industry-specific questionnaires to uncover cyber and business risks introduced to the enterprise. This feature should also take advantage of shared community assessments, which can provide insight into new vendors, according to how other organizations rated that vendor.

### *Vendor Risk Assessments*

Developing a security posture for a vendor typically involves manually reviewing spreadsheets of vendor-answered questions. Commercial solutions should automate the data collection and risk assessment process, thus easing manual review burdens of security teams. Commercial vendors should offer prepackaged assessments, including support for the NIST, ISO, CSA, HIPAA and PCI compliance frameworks, and should include a built-in risk analysis model and remediation recommendations for vendors.

### *Vendor Risk Monitoring*

The commercial platform should review external sources to proactively identify risks to avoid situations like the SolarWinds Orion issue. Functions should be included to support discrete monitoring of the dark web, public threat feeds and private threat feeds. Such capabilities can help to identify and alert about third-party breaches quickly, as well as to validate assessment responses.

### *Vendor Performance and SLA Management*

One of the most challenging aspects of monitoring vendor performance and service levels is developing metrics. This detail is often deferred until after a contract has been signed, leaving many organizations challenged to measure the services they purchased. Functionality should be included to provide for the definition of SLAs during contracting, thus ensuring that measurement throughout the vendor lifecycle is part of the contract per agreed-upon service levels.

### *Vendor Offboarding and Termination*

After years of relying on a vendor, enterprises typically struggle with the risks associated with contract termination. Scope creep, implementation of additional features and personnel churn create risk to both operations and shared data. A feature should be included to provide insight into contract enhancements, data sharing agreements and security assessments, thus enabling IT staff to programmatically review end-of-relationship tasks and operational changes to mitigate overall data security risk.

## **MAPPING PREVALENT TO THE FOUNDATIONAL RISK MODEL**

The Prevalent solution matches up well with the foundational model discussed earlier in this paper by addressing reduction in both likelihood and consequences for the various components of the framework. Major elements of the coverage mapping are listed below:

*Vendor Sourcing and Selection*—The Prevalent platform can manage the procurement lifecycle from vendor selection and risk analysis via their risk intelligence network, and through the third-party vendor selection and contracting process, using a solution called Contract Essentials.

*Centralized Vendor Onboarding*—Prevalent does validate requirements, enforce legal constraints and ensure that the contract is managed correctly. Also, the information security and risk teams can review vendor-related technology risks by mapping interrelationships in the platform.

*Inherent Risk Scoring*—Prevalent's inherent risk scoring features allow for custom, business or industry-specific questionnaires to uncover cyber and business risks introduced to the enterprise. This feature also takes advantage of Prevalent's shared community assessments. The outcome is a clearer picture of what risks to drill into further.

*Vendor Risk Assessments*—Prevalent automates the data collection and risk assessment process, easing manual review burdens of security teams. Prevalent comes with over 75 prepackaged assessments, including support for the NIST, ISO, CSA, HIPAA and PCI compliance frameworks.

*Vendor Risk Monitoring*—Prevalent reviews external sources to proactively identify risks to avoid situations like the SolarWinds Orion issue. Prevalent monitors the dark web, public and private threat feeds, thousands of .onion and criminal sites, and formal government and community repositories.

*Vendor Performance and SLA Management*—Prevalent's SLA and performance management functionality provides for the definition of SLAs during contracting, thus ensuring that measurement throughout the vendor lifecycle is part of the contract per agreed-upon service levels.

*Vendor Offboarding and Termination*—The Prevalent offboarding feature provides insight into contract enhancements, data sharing agreements and security assessments, thus enabling IT staff to programmatically review end-of-relationship tasks and operational changes to mitigate overall data security risk.

The coverage mapping for the Prevalent solution is shown in Figure 3.

Enterprise teams might perform the mapping differently from the solution in Figure 3, but the general concept should remain constant—namely, that Prevalent platform functions line up well with probability and consequences reduction. Take, for example, the support provided by the vendor sourcing and selection function. This capability reduces all aspects of the risk model by including automated support for vendor management throughout the lifecycle.

Third-Party Cyber Risk	Prevalent Function Influencing Probability	Prevalent Function Influencing Consequences
<b>Software</b>	Vendor Sourcing and Selection, Inherent Risk Scoring, Vendor Risk Assessments, Vendor Risk Monitoring	Vendor Sourcing and Selection, Inherent Risk Scoring, Vendor Risk Assessments, Vendor Risk Monitoring
<b>Compliance</b>	Vendor Sourcing and Selection, Centralized Vendor Onboarding, Vendor Risk Assessments, Vendor Risk Monitoring, Performance and SLA Management, Offboarding and Termination	Vendor Sourcing and Selection, Centralized Vendor Onboarding, Vendor Risk Assessments, Vendor Risk Monitoring, Performance and SLA Management, Offboarding and Termination
<b>Fraud</b>	Vendor Sourcing and Selection, Vendor Risk Assessments, Vendor Risk Monitoring	Vendor Sourcing and Selection, Vendor Risk Assessments, Vendor Risk Monitoring
<b>Responsibility</b>	Vendor Sourcing and Selection, Vendor Risk Assessments, Vendor Risk Monitoring, Performance and SLA Management	Vendor Sourcing and Selection, Vendor Risk Assessments, Vendor Risk Monitoring, Performance and SLA Management
<b>International</b>	Vendor Sourcing and Selection, Vendor Risk Assessments, Vendor Risk Monitoring	Vendor Sourcing and Selection, Vendor Risk Assessments, Vendor Risk Monitoring
<b>Complexity</b>	Vendor Sourcing and Selection, Inherent Risk Scoring, Vendor Risk Assessments, Vendor Risk Monitoring	Vendor Sourcing and Selection, Inherent Risk Scoring, Vendor Risk Assessments, Vendor Risk Monitoring

Figure 3. Mapping Prevalent Functions to Foundational Risk Model

## PROPOSED ACTION PLAN FOR ENTERPRISE BUYERS

Enterprise security and risk management teams should create an action plan immediately to improve their third-party cyber risk management capability. This should include:

1. inventorying existing third-party risk solutions;
2. matching up existing solutions against the foundational risk model introduced here to determine gaps; and
3. selecting and using a platform solution that can address any aspects of third-party cyber risk that include insufficient coverage.

The review and selection of a suitable third-party security vendor will benefit from the following questions to be asked during the buying process, and easily included in the request for proposal (RFP) materials shared with vendors such as Prevalent:

- *Does your solution address both probability and consequences of cyber risk—and if so, how is this performed?*
- *Does your solution line up well with the tangible third-party risks associated with software, compliance and fraud—and if so, how is this performed?*
- *Does your solution address the third-party risks associated with shared responsibility, international requirements and complexity—and if so, how is this performed?*

Not all vendors will cover the full model, as should become evident using the questions listed above. The enterprise must ensure coverage, however, and this can be achieved through a single platform, as illustrated by Prevalent, or through the use of multiple vendors with more isolated focus. Each approach has pros and cons. A unified platform, for example, avoids seams, whereas multiple tools allow for the use of some new future innovation that might emerge.

## APPENDIX A: ADDITIONAL SELECT NON-CYBERFEATURES SUPPORTED BY THE PREVALENT PLATFORM

Capability	Description
Antibribery/Anti-corruption (ABAC) and Corporate Ethics	Ensures vendor compliance with the U.S. Foreign Corrupt Practices Act (FCPA) and the U.K. Bribery Act, as well as continual adherence to corporate ethics requirements.
Contract Lifecycle Management	A fully SaaS solution that enables parties from all parts of the contracting process to share, comment on and review vendor contracts.
Diversity	Automates vendor diversity and hiring practice assessments.
Corporate Environmental, Social and Governance (ESG)	Automates vendor ESG assessments to ensure that third parties are in line with the corporate ESG direction.
Modern Slavery	Automates vendor assessments pertaining to the Australian, U.K., and U.S. regulations on visibility into slavery and human trafficking within the supply chain.
Precontract Due Diligence	Provides instant access to hundreds of thousands of prefilled reputational and financial vendor risk profiles.
Reputational and Financial Monitoring	Adds continual monitoring of private and public records to identify changes in vendor risk profiles.
Supply Chain Resilience	Performs vendor assessments around business continuity, crisis management, pandemic planning, environmental disasters and other supply chain disruptions.

<sup>1</sup> <https://www.verizon.com/business/resources/articles/third-party-vendor-risk-management/>

<sup>2</sup> Homeland Security Emergency Directive 21-01: SolarWinds Orion Code Compromise

<sup>3</sup> This section was developed with technical guidance from Prevalent (<https://www.prevalent.net/>), which provides a commercially available third-party risk management platform. Prevalent's guidance was used to generalize a set of suitable functional requirements that match up with our foundational model for third-party risk.

# INTEGRATING CYBERSECURITY SUPPORT FOR HOME AND SMALL BUSINESS INTO TELECOM SERVICE INFRASTRUCTURE

EDWARD AMOROSO

---

Home and small business users in the U.S. market are poorly served today with ad hoc and unconnected cyberprotections. Telecom providers are thus advised to address this challenge by integrating security support for home and small business customers into their service infrastructure. Such integration can be accomplished through the deployment of functional controls into the core network, premise routers and endpoints. A commercially available platform<sup>1</sup> is shown to effectively support such cybersecurity solution integration.

## OUTLINE

- 1. Introduction
- 2. Cybersecurity for the Home
  - 2.1 Cybersecurity Solutions
    - 2.1.1 Content Filtering
    - 2.1.2 Virus Protection
    - 2.1.3 Device Security
    - 2.1.4 Identity Protection
    - 2.1.5 Financial Protection
    - 2.1.6 Credential Security
  - 2.2 Analysis of Cybersecurity Solutions for the Home
- 3. Cybersecurity for the Small Business and Microbusiness
  - 3.1 Cybersecurity Solutions
    - 3.1.1 Security Compliance
    - 3.1.2 Data Security
    - 3.1.3 Reputation Protection
    - 3.1.4 Third-Party Security
    - 3.1.5 Network Security
    - 3.1.6 Account Protection
  - 3.2 Analysis of Cybersecurity Solutions for the Small Business and Microbusiness
- 4. Traditional Service Providers' Free Cybersecurity Features
  - 4.1 Cybersecurity Features From ISPs
    - 4.1.1 Fraud Detection

4.1.2 Spam Filtering	6.2.2 Premise Router Security
4.1.3 Encryption	6.2.3 Endpoint Security
4.1.4 Security Analytics	6.3 Go-to-Market Plan
4.1.5 Traffic Management	7. Overview of the Allot Platform
4.1.6 Network Monitoring	7.1 Allot Customer Base
4.2 Analysis of Cybersecurity Features From ISPs	7.1.1 Telefonica
5. Traditional Service Providers' Cybersecurity Service Offerings	7.1.2 DISH
5.1 Cybersecurity Offerings From ISPs	7.1.3 Safaricom
5.1.1 Web Security Services	7.1.4 Rakuten
5.1.2 Email Security Services	7.1.5 Exetel
5.1.3 DDoS Security	7.1.6 Eolo
5.1.4 PKI Services	7.1.7 Vodafone
5.1.5 Managed Security Services (MSS)	7.2 Allot Services Overview
5.1.6 Consulting Services	7.2.1 HomeSecure
5.2 Analysis of Cybersecurity Offerings From ISPs	7.2.2 EndpointSecure
6. Extending the Telecom Service Provider Platform for Cybersecurity	7.2.3 NetworkSecure
6.1 Telecom Security Value Proposition	7.2.4 IoTSecure
6.1.1 Value Proposition for Home Customers	7.2.5 DDoS Secure
6.1.2 Value Proposition for Small Business and Microbusiness Customers	8. Sample Business Case for Telecom Service Providers
6.2 Telecom Options to Provide Security to Home and Small Business Customers	8.1 Sample Business Case Development
6.2.1 Core Network Security	8.2 Sample Revenue Estimates
	8.3 Sample Cost Estimates
	8.4 Sample Income Statement

## 1. INTRODUCTION

In the early days of information security, computer-related threats were viewed almost exclusively from the perspective of business, government and military groups. This was appropriate, since computing was done primarily in these contexts—so any type of malicious hacking would target organizational assets exclusively. Most security controls thus focused on serving business and government, as in, for example, data encryption products for banks.

As individuals, homes and small businesses went online, commercial tools emerged that were designed to help citizens protect their data. Antivirus software was the first successful offering, with companies such as Symantec and Norton selling software to protect Windows PCs from viruses.<sup>2</sup> Hackers soon found their way around this signature approach, but the foundation was created for security software being used in the home.

Today, the cybersecurity marketplace has become a growing and vibrant aspect of modern business, with a wide variety of choices for organizations to protect their resources. Interestingly, however, the options for individuals, homes and small businesses have not changed much since the early days. Most citizens still rely on weak antivirus products that are ineffective in protecting against ransomware, identity theft and inappropriate content.

This report outlines a strategy for serving this market<sup>3</sup> through advanced security capabilities embedded into telecommunication provider infrastructure. The resulting platform would include advanced security

for home and small business users and can extend to protect family members from undesirable content. A commercially available platform is used to explain this approach and to serve as a basis for how such embedded security can be delivered.

## 2. CYBERSECURITY FOR THE HOME

The modern home user requires a range of security protections for their data, systems and access. Such protection extends to work-from-home initiatives, advanced by the recent pandemic and by general trends toward employees choosing to work in more flexible day-to-day arrangements. Home cybersecurity thus involves a collage of different requirements and needs, based on the specifics of the family being supported.

### 2.1 Cybersecurity Solutions

A key aspect of current cybersecurity solutions for family and home users is that they are offered on an ad hoc basis, with little support for customers to develop a coherent protection strategy. Instead, they must select from a wide range of options from many different sources, with no guidance on whether the security features even work. The functional requirements for cybersecurity solutions in the home today can be grouped into the following major categories:

Typical U.S. homes will also include family members who are employees of companies, so it is likely that they use an installed VPN client on their PC or other company-provided access tools to gain entry to the corporate network.<sup>4</sup> While this type of infrastructure is likely to be provided directly by the employer, it does introduce the issue that a family member might have certain endpoint or network requirements imposed by their company. An obvious example would be the use of a company-issued PC by a family member as their primary device.

#### 2.1.1 Content Filtering

This involves avoidance of access to undesirable content either through direct or URL-redirected connections. This is usually done by specialized overlay software or tools for the PC or mobile device. Verizon, for example, resells the Mobicip solution for iPhone users to keep families safe from undesirable

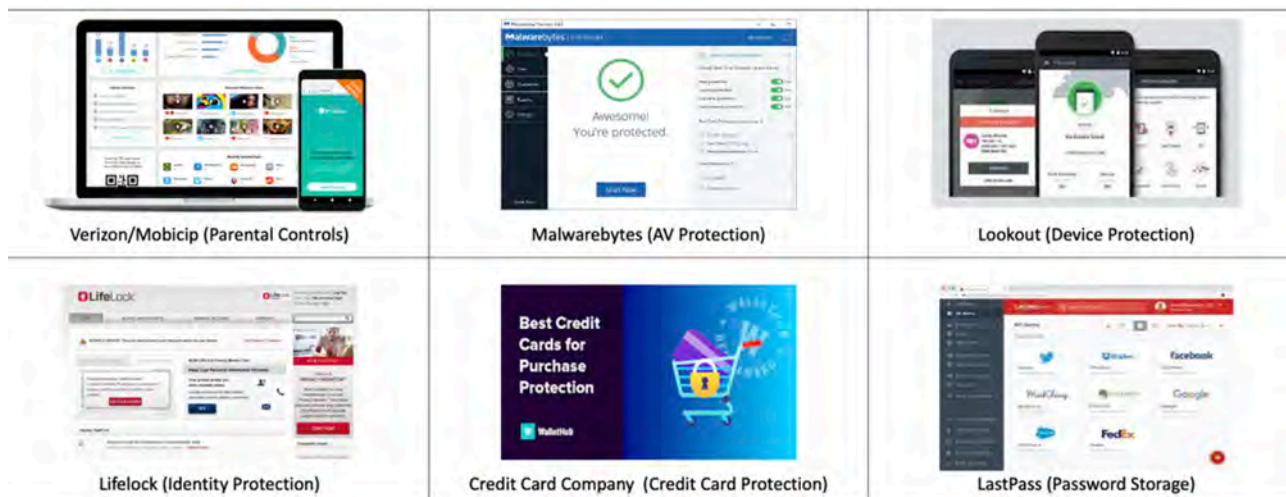


Figure 2.1-1. Potential Security Services in a Hypothetical U.S. Family and Home

**Key Point:** Current cybersecurity solutions for family and home users are offered on an ad hoc basis, with little support for customers to develop a coherent protection strategy.



content.<sup>5</sup> Comcast embeds content filtering in its Xfinity service offering into routers guided by a mobile app.<sup>6</sup> The options for most families are complex and require administration so that parents are not subjected to the same controls as children.<sup>7</sup>

### *2.1.2 Virus Protection*

This includes prevention from the harmful effects of malware that enter PCs and other devices, usually through phishing. Home users typically download an antivirus solution such as Malwarebytes to their Windows PC (still a high percentage of the market).<sup>8</sup> Fewer users download antivirus tools to Mac computers, thanks to embedded controls.<sup>9</sup> Determination of whether these tools work is difficult, and most home users would express dissatisfaction with their existing virus controls for the PC.<sup>10</sup>

### *2.1.3 Device Security*

This involves protection of mobile devices such as smartphones and tablets from any malware or other integrity issues that can affect the device operation. Many companies market security solutions for Android devices and iPhones. These offerings usually combine antivirus with features such as locating a lost or stolen device.<sup>11</sup> Considerable confusion exists in the U.S. market regarding whether an iPhone (or Android) device needs additional security protection beyond what is offered by the manufacturer.<sup>12</sup>

### *2.1.4 Identity Protection*

This includes prevention of unauthorized access to identity-related information such as Social Security numbers in the U.S. Home and small business users typically obtain such protection from identity services such as Identity Guard, IdentityForce and LifeLock.<sup>13</sup> Identity services are often provided as a compensatory act by service providers after a breach.<sup>14</sup> Mainstream media includes articles on recommended identity security solutions, which often include monthly fees (e.g., \$30-\$35 per month) that can be a challenge for some budgets.<sup>15</sup>

### *2.1.5 Financial Protection*

Such protection is designed to help avoid loss of financial data such as credit cards, bank accounts and similar information. Buyers usually obtain these services from their financial institution or credit card company, but the threat continues to be significant.<sup>16</sup> While this is technically not a cybersecurity control, many homes and small businesses view this as an extension of their overall online protection.

### *2.1.6 Credential Security*

This involves protection of account credentials to online services, social media accounts and email. Some home users utilize password managers such as Keeper or LastPass, but these are not widely deployed to families.<sup>17</sup> Many families are more likely to just write down passwords, and even to share common passwords and other account information to avoid multiple fees to services such as Netflix.<sup>18</sup> Hacked Facebook and other social media accounts are a common complaint for many family members.<sup>19</sup>

## *2.2 Analysis of Cybersecurity Solutions for the Home*

The bottom line for home and family users is that security solutions are (1) not well-integrated; (2) offer unclear benefits, with confusing metrics about effectiveness; and (3) come from a variety of different, unconnected sources, including service providers, banks and security companies. Many buyers end up purchasing a few of these services and not taking full advantage of the free capabilities that come with their existing purchases.

The opportunity for telecom providers to offer a simple, clear package of cybersecurity protections for homes and families appears significant, especially given the attention in the media regarding increased cyber risk to the home. While it is unlikely that telecom providers could cover every use case,

many of the online protections that are purchased in an ad hoc manner could be integrated into the services from the ISP. The scale and scope of most domestic ISPs can also serve to keep prices reasonable.

**Key Point:** Cybersecurity solutions for homes and families are not well-integrated, offer unclear benefits, and come from a variety of different, unconnected sources.

### 3. CYBERSECURITY FOR THE SMALL BUSINESS AND MICROBUSINESS

The modern small business and microbusiness also require a range of security protections for their data, systems and access. Such protection can come from company founders and leaders desiring better security, or it can be imposed as a requirement from customers. Small business and microbusiness cybersecurity thus also involves, as with home users, a collage of requirements and needs based on the specifics of the company.

Like home and family users, small businesses and microbusinesses must contend with ad hoc and nonintegrated security solutions from a variety of different sources. This includes security features for all the SaaS and cloud services being used, as well as banking and financial support services from banks and credit card companies. The result is a complex cybersecurity product and services market for small businesses and microbusinesses, which are increasingly being targeted by malicious actors.<sup>20</sup>

#### 3.1 Cybersecurity Solutions

The functional requirements for cybersecurity for small businesses and microbusinesses include all the issues listed above for homes. Every small business, for example, must avoid viruses on their PCs. In addition to these baseline security concerns, small businesses and microbusinesses have additional security requirements that can be grouped into the following major categories.

##### 3.1.1 Security Compliance

This includes various security compliances that must be met, including Payment Card Industry (PCI) Data Security Standard (DSS). Payment providers are often prominent partners helping small businesses to establish the right compliances. Visa offers an extensive list of global service providers

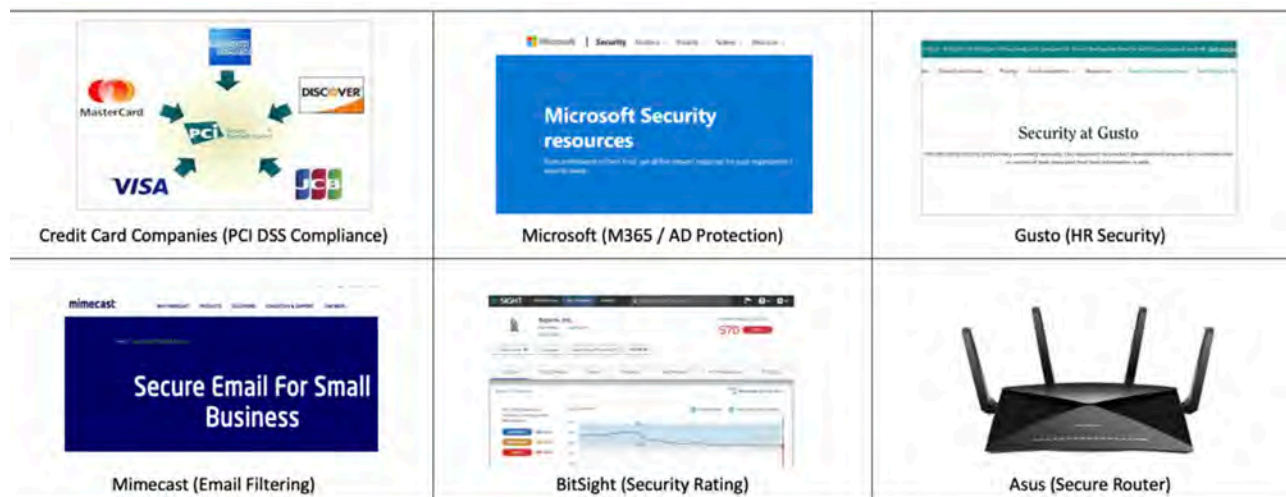


Figure 3.1-1. Potential Security Services in a Hypothetical U.S. Small Business

**Key Point:** Like home and family users, small businesses and microbusinesses must contend with ad hoc and nonintegrated security solutions from a variety of different sources.

that offer merchant support, payment facilitation and other services.<sup>21</sup> Such compliances are established by having the small business fill out an annual questionnaire.

### *3.1.2 Data Security*

This requirement involves avoiding customer data theft or loss due to unauthorized access as part of an attack or malware. Some security vendors, such as AaDya, focus on offering monthly support in this area for small business.<sup>22</sup> Larger banks, credit card companies (e.g., American Express) and SaaS providers (e.g., Microsoft) also offer resource centers and security support.<sup>23</sup> The requirement also involves avoiding employee data theft or loss (e.g., salary information) due to unauthorized access as part of an attack or malware. This is generally accomplished through the available security features of SaaS tools that manage employee data such as online HR services (e.g., Gusto).<sup>24</sup>

### *3.1.3 Reputation Protection*

This involves the protection of the reputation and brand of small businesses and microbusinesses from fraudulent activity. This is often done through support from an email security provider, such as Mimecast (to include DMARC records).<sup>25</sup> Many articles and online resources exist to help small businesses to follow checklists to secure their brand.<sup>26</sup> Brand and reputation management on social media is a likely growth area for small business and microbusiness customers.

### *3.1.4 Third-Party Security*

This includes support for small business and microbusiness third parties that must demonstrate proper security to one of their larger customers. The use of security ratings services is now common for small business (e.g., Security Scorecard or Bitsight),<sup>27</sup> and exchanges are now emerging for small businesses to register their security posture.<sup>28</sup> Most large companies designate small businesses and microbusinesses into a special tier and will lessen the intensity of questionnaires and other requirements to include simple controls such as proof of awareness training and evidence of an incident reporting policy.

### *3.1.5 Network Security*

Prevention of attacks or unwanted access to business networks, including any Wi-Fi or other network systems, is a concern for small business. This is typically done by landlords such as WeWork<sup>29</sup> who control Wi-Fi access for their tenants (often not well).<sup>30</sup> It can also be done through the basic settings on the local access or Wi-Fi router that a small business might set up in any shared space. Work-from-home access is controlled by the individual employees in their homes, also through administration of their router and Wi-Fi access point.<sup>31</sup>

### *3.1.6 Account Protection*

This includes assurance that all SaaS, cloud and web application accounts are protected and managed to avoid unauthorized access. Many guidelines exist to help small businesses check the security settings of their SaaS capabilities.<sup>32</sup> Some services, such as Siriux, have emerged to scan the settings of Microsoft 365, which is commonly used by small businesses and microbusinesses.<sup>33</sup>

## *3.2 Analysis of Cybersecurity Solutions for the Small Business and Microbusiness*

The bottom line for small business and microbusiness users is that available security solutions in the U.S. are (1) not well-integrated; (2) offer unclear benefits; and (3) in some cases are materially nonpresent. In many cases, such as with Microsoft and most SaaS offers, the security features come with the service being used, which implies no additional spend by the customer.

Similarly, MFA solutions such as Google Authenticator are also popular with small businesses, because they involve no fees.<sup>34</sup>

The opportunity for U.S. telecom providers to offer a simple, clear package of cybersecurity protections for small business and microbusiness appears significant, especially given the attention in the media regarding increased cyber risk. While it is unlikely that telecom providers could cover every use case for small business, many of the online protections that are purchased in an ad hoc manner could be integrated into the services from the ISP. The scale and scope of most domestic ISPs can also serve to keep monthly business expenses reasonable.

**Key Point:** The opportunity for U.S. telecom providers to offer a simple, clear package of cybersecurity protections for small business and microbusiness appears significant.

## 4. TRADITIONAL SERVICE PROVIDERS' FREE CYBERSECURITY FEATURES

To address cyberthreats to users of broadband internet access and 4G/5G wireless services, telecom providers have traditionally included certain capabilities in the core of their network infrastructure. Note that home and small business customers primarily purchase broadband internet access and wireless telephony. Larger businesses also purchase private network support, consulting, managed services and other offerings. The features listed below are free.

It is worth differentiating between broadband (fiber, wired) services and wireless (4G, 5G) service infrastructure. While both include embedded security features, wireless services are increasingly software-defined, which offers excellent opportunities to integrate new virtual controls into the service environment. This is especially true for 5G services, which can include a variety of prevention, detection and response capabilities embedded into both the core and radio access. RAN slicing at the tower, for example, is a powerful feature for separating groups of wireless users.<sup>35</sup>

**Key Point:** To address cyberthreats to broadband and wireless customers, telecom providers have traditionally included security capabilities in the core of their network infrastructure.

### 4.1 Cybersecurity Features From ISPs

The primary core capabilities that telecom providers have embedded into their core operations have not traditionally been revenue generators, but rather enhance the overall service experience for both users and the provider. These capabilities are typically guided by legal and privacy constraints, which are intended to ensure that telecom providers are not being too aggressive in their security actions.

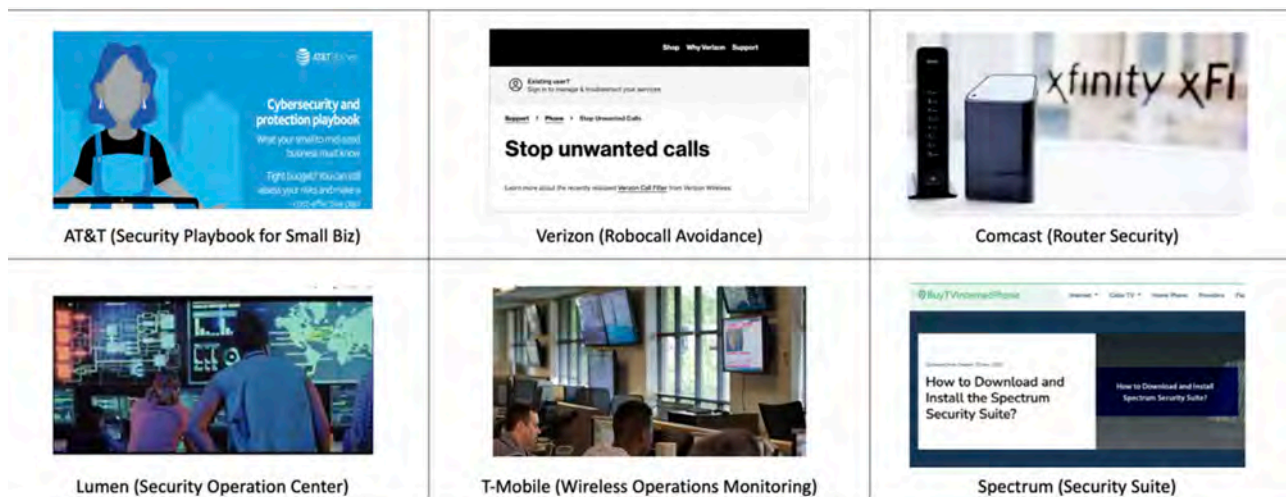


Figure 4.1-1. Collage of Typical Free ISP Security Features

It cannot be emphasized enough, however, that in the U.S. market, telecom service providers must address trust concerns that large segments of buyers have with their ISP. Embedded security services will have to be explained carefully so that end users do not have worries that their activity is being monitored or wiretapped. Political issues concerning the role of the service provider have also complicated this relationship between ISPs and customers.<sup>36</sup>

One useful observation that can be made by service providers is that they reduce the number of third parties that might be involved in managing data. While this is more concerning to larger customers than smaller ones or consumers, it is nevertheless true for all subscribers. This argument has not been a prominent issue in the trust debate, but it might be a useful strategy for communications service providers in the future.

#### *4.1.1 Fraud Detection*

The identification of fraud patterns in telephony has been a core competency of telecoms for many decades. AT&T has always included fraud detection for its core telephony, and this now includes protection against robocalls and unwanted mobile calls.<sup>37</sup> ISPs also offer online articles, tips and guidance for dealing with this problem.<sup>38</sup>

#### *4.1.2 Spam Filtering*

This protection includes filtering a significant portion of spam that enters a telecom provider's backbone with the use of automated detection systems. These algorithmic techniques are well-known and have been in place for many years.<sup>39</sup> Service providers of email such as Google also do a large portion of the spam filtering.<sup>40</sup> Google's advertisements about its security protection for Gmail users have been quite aggressive, including multiple pages in *The Economist* every month.<sup>41</sup>

#### *4.1.3 Encryption*

This protection comes with wireless services that have progressed toward 5G to include strong encryption solutions between handsets and towers (although this is not perfect).<sup>42</sup> Encryption support also ships with most ISP broadband routers for WEP support.<sup>43</sup> Over-the-top encryption apps for voice, such as from Silent Circle, are available but not extensively used by families or small business.<sup>44</sup> Even larger companies with traveling corporate executives have not been extensive users of these voice encryption apps, presumably because they trust the underlying telecom provider for security. This is not a good assumption in some countries where the government regularly monitors activity.<sup>45</sup>

#### *4.1.4 Security Analytics*

Telecoms use security analytic tools to review traffic for evidence of worms, botnet attacks and other visible attacks.<sup>46</sup> This processing activity is hidden from most end users, but it does offer backbone protection. During the early 2000s, this work was useful in protecting against the cascading of internet worms.

#### *4.1.5 Traffic Management*

The management and route shaping of traffic is performed by service providers to ensure that communications are not inappropriately diverted (e.g., to a country).<sup>47</sup> This is also hidden from most end users but does offer some useful security protection.

#### *4.1.6 Network Monitoring*

It is common for telecom service providers to perform network monitoring of their core network or extended access infrastructure, including for wireless 4G/5G. This work is often done in search of some known attack signature (e.g., evidence of a botnet), or for other evidence (e.g., law enforcement-required, as with CALEA).<sup>48</sup> This is also hidden from most end users but does provide additional security protection.

#### 4.2 Analysis of Cybersecurity Features From ISPs

The bottom line for typical ISP security features is that they are not well-known and are largely hidden from their end users. Historically, U.S. users have also not responded well to ISPs watching their browsing activity, presumably for the purpose of marketing.<sup>49</sup> In addition, there have been big lawsuits based on accusations that ISPs are being too aggressive in monitoring network communications in conjunction with U.S. intelligence and law enforcement.<sup>50</sup>

The prior challenges that ISPs have had in marketing their security features is an important consideration for telecoms that choose to embed protections into their network for home and small business protection. Extensive outreach and marketing campaigns will be required to help users understand the purpose of the protection, how it works, and why it would not represent a privacy or trust issue. Many popular articles have emerged that accuse domestic ISPs of spying on their users. This perception would have to be managed.<sup>51</sup>

**Key Point:** Outreach campaigns will be required to help users understand the purpose of telecom security protections, including how they work and why they do not affect privacy.

## 5. TRADITIONAL SERVICE PROVIDERS' CYBERSECURITY SERVICE OFFERINGS

Telecom providers have had the challenge of balancing the needs of their service obligations to deliver customer traffic from senders to recipients, with the need to help prevent hacking and other threats. This has always been a major challenge, and it has been addressed to date by offering contractual terms to customers to help support their security needs. This has been done primarily through paid managed security solutions, often to larger business customers.

Accordingly, over the past decade or so, virtually every telecom provider in the U.S. has developed a managed security business. This began with simple remote up-down management of firewalls on internet gateways, but it has now evolved into full implementations of managed detection and response (MDR), network detection and response, and extended detection and response (XDR) services.<sup>52</sup> No one ISP has come to dominate the market, but all appear to have significant revenue to warrant continued support from upper management.

### 5.1 Cybersecurity Offerings From ISPs

The traditional provision of cybersecurity from telecom providers to the home user, and to small businesses and microbusinesses, has been less clear over the past two decades than such provision to larger businesses and government agencies. Most telecoms, in fact, have significant security businesses in the managed services and consulting arenas. Verizon, for instance, publishes a popular Data Breach Investigations Report (DBIR) each year.<sup>53</sup> The Verizon DBIR is marketed to larger companies. Business services from telecoms to enhance security can be grouped into the following major categories:

#### 5.1.1 Web Security Services

This includes secure web gateway (SWG) services designed to avoid malware from infected sites by proxying services for URL filtering. Cisco Umbrella and WebTitan are two typical (and popular) secure web gateways that are marketed to small businesses.<sup>54</sup> Locally managed content filtering packages are also available from various software companies and SaaS solution providers.<sup>55</sup> Many security services are also available for schools to filter undesirable content from student access.<sup>56</sup>

#### 5.1.2 Email Security Services

This category focuses primarily on the filtering and offline review of suspicious content attachments

and potential phishing links in email. Comcast Business SecurityEdge is an example of an ISP offering for small business that is focused on protection of email from phishing and related attacks.<sup>57</sup> Microsoft and Google also include email filtering for their mail services, although these capabilities often work differently on PCs and mobile devices.

### *5.1.3 DDoS Security*

This control is designed to divert layer 3 denial-of-service (DDoS) attacks to special scrubbing complexes.<sup>58</sup> This type of service is more likely to be subscribed to by larger businesses. Small businesses are rarely concerned with DDoS attacks.

### *5.1.4 PKI Services*

This type of service involves support for e-commerce, and it often includes provision of a signed certificate for websites desiring to run the HTTPS protocol. Hosting providers such as GoDaddy, for example, have offered popular PKI services in support of new businesses signing up for web hosting.<sup>59</sup> Support for secure e-commerce is an important aspect of protection for small businesses and many other organizations, such as banks. Articles are available to help small operators secure their website for selling products online.<sup>60</sup> Guidance ranges from the recommendation to use HTTPS to advice about including website monitors.<sup>61</sup>

### *5.1.5 Managed Security Services (MSS)*

This category includes a range of managed services for security devices such as firewalls and intrusion detection systems. Lumen (i.e., CenturyLink) offers a typical range of services in this area.<sup>62</sup> This type of service is more likely to be subscribed to by larger businesses. Most ISPs include a significant MSS offering, and smaller managed service providers (MSPs) have begun to include security as a part of their service to their local and regional customers. Many vendors market their protection platform to MSPs to help them grow their revenue by including managed security services such as scanning, antivirus and other protections.<sup>63</sup>

### *5.1.6 Consulting Services*

This involves consulting guidance from experts for cybersecurity issues affecting business customers, usually larger ones. Most small businesses obtain this type of assistance from services such as the Geek Squad from Best Buy<sup>64</sup> or the Genius Bar from Apple.<sup>65</sup> Small businesses and microbusinesses also tend to get their consulting and managed security advice from their local MSP, often set up regionally and typically colocated geographically with the small business and the microbusiness being supported.<sup>66</sup>

## *5.2 Analysis of Cybersecurity Offerings From ISPs*

The bottom line for typical ISP security offerings is that they have tended to skew toward larger customers with security teams and budgets. These services include tiered support that requires enough security knowledge on the part of the customer that dedicated IT or security team members become a requirement to purchase and use the services. This tends to make services such as firewalls and web security impractical for small businesses and microbusinesses.

Most MSPs do include security services now for small business and microbusiness customers, and this represents an available channel today for how these entities obtain their protections. Regional MSPs often have the advantage of local relationships with their customers (e.g., small businesses, municipal departments, schools, police departments) and are often the main source of information and support for cybersecurity. This should be a consideration for ISPs that are moving in the direction of adding more security protection to their core infrastructure. They will need to strategize how these services can be included in MSP offerings.

Security consulting services from ISPs have not been prominent for small business, but rather have

been obtained through resource centers or online FAQs. ISPs have tended to avoid dealing with the day-to-day issues of customer PC problems, software issues and other localized problems from their help desks. The Best Buy Geek Squad and the Apple Genius Bar offer security consulting services as a complement to their retail offerings and to improve the overall experience of customers visiting their stores.<sup>67</sup> ISPs should view this as an opportunity to expand their own services.

**Key Point:** Typical telecom cybersecurity offerings have tended to skew toward larger customers with in-house enterprise security teams and significant budgets.

## 6. EXTENDING THE TELECOM SERVICE PROVIDER PLATFORM FOR CYBERSECURITY

Telecom service providers have the following advantages with respect to the provision of cybersecurity solutions for homes and small businesses: (1) existing business relationships with monthly paid accounts and service support; (2) inline connectivity, where the network provides an essential aspect of the device-to-app use case for most families and businesses; and (3) ability to scale the service to the massive market for homes and small business.

Domestic U.S. telecom companies are thus well-positioned to extend their service offerings to include security support for these important customer segments. With recent increases in publicized threats to the home and small business, the time is right in 2022 for these services to become more prominently marketed and more aggressively sold through existing retail and sales account channels.<sup>68</sup>

### 6.1 Telecom Security Value Proposition

Telecoms must clearly define their value proposition for cybersecurity services extended to the home and small business. Such value propositions must establish trust that the telecom's purpose is to protect the customer and not to support some larger objective related to marketing or law enforcement coordination.<sup>69</sup> While value propositions will differ from one telecom to another, each statement should be rooted in the following key points (expressed as statements from the telecom to their customer):

- Positioning—"As your telecom, we support your communications today. Extending this support to security is a natural progression. We are well-positioned to help you avoid malware and unwanted content."
- Billing—"As your telecom, we already have a monthly billing arrangement with you. Extending this billing process to include security will save you the time and effort of dealing with other vendors."
- Resources—"As a large organization, we have the resources to pick and choose the right security tools for you. This helps you avoid the need to differentiate between hundreds of confusing options."

**Key Point:** Telecoms must clearly define the specific value propositions for security services extended to the home, small business and microbusiness customer.

#### 6.1.1 Value Proposition for Home Customers

The value proposition for securing home customers must be tailored to meet the needs of U.S. families—and any telecom would be wise to query their customer base with local research. Patterns of behavior and attitudes vary significantly in the U.S., especially with the so-called red/blue split in the country.<sup>70</sup> A family in Tennessee, for example, is likely to list requirements different from those of a family in Brooklyn. These differences are sufficiently great to warrant tailored marketing and local research by the ISP.



Nevertheless, the primary value propositions for home customers should be rooted in the following key points (expressed as statements from the telecom to their home customer):

- Children—“We know that you are concerned with the content that your children might be exposed to on the internet. As your ISP, we can make sure that this is appropriately managed in a way that can only be bypassed by you, the parent.”
- Malware—“We know that you are concerned that malware might find its way onto your home PCs over your network connection. As your ISP, we can help filter this malware to ensure that you are safe.”
- Effort—“We know that you are too busy to have to expend effort each day to manage your security. As a large organization, we have the resources to do this for you.”

**Key Point:** The value proposition for home customers must be tailored to meet the needs of U.S. families, which will vary according to region.

### 6.1.2 Value Proposition for Small Business and Microbusiness Customers

The value proposition for securing small business and microbusiness customers cannot simply be downsized from that of larger enterprise customers. Instead, the value proposition must match up with the highly distributed, highly virtualized nature of small business, with its increasingly intense use of cloud and SaaS-based services. Small businesses in the U.S., including ones not traditionally associated with IT or deep computer skills, are now leveraging online services (e.g., M365, QuickBooks) to improve their operation.<sup>71</sup>

It is also worth pointing out that wide swings of concern exist between the tiniest microbusiness, perhaps one person working from the home, to a small business of 50 or so employees operating from a dedicated business location, perhaps with a private local area network (LAN).<sup>72</sup>

In both cases, the likelihood that employees spend a great deal of time working from home is significant. But perhaps the biggest business difference between the two is that to grow profits, many small businesses will work to minimize their expenses. Microbusinesses tend to already have low or zero operating expenses, so their only path to increased profitability will be to grow revenue. From a security perspective, the biggest difference is that a small business is likely to include at least some person or small group that focuses on IT, computers, networks and security. Microbusinesses will have absolutely zero security support and will rely on the Apple Genius Bar, Best Buy Geek Squad, or family or local connections for security assistance.

Accordingly, the primary value propositions for small businesses and microbusinesses should be rooted in the following key points (expressed as statements from the telecom to their customer):

- Threats—“We know that you are concerned with online threats, but not sure how to address this challenge. As your ISP, we can make sure that you are properly covered.”
- Cost—“We know that you have a limited budget to spend on cybersecurity. We will make sure that your monthly fees are reasonable and integrated into your existing telecom bill.”
- Effort—“We know that you are too busy running your business to expend effort each day to manage your security, or to hire someone to do this work. As a large organization, we have the resources to do this for you.”

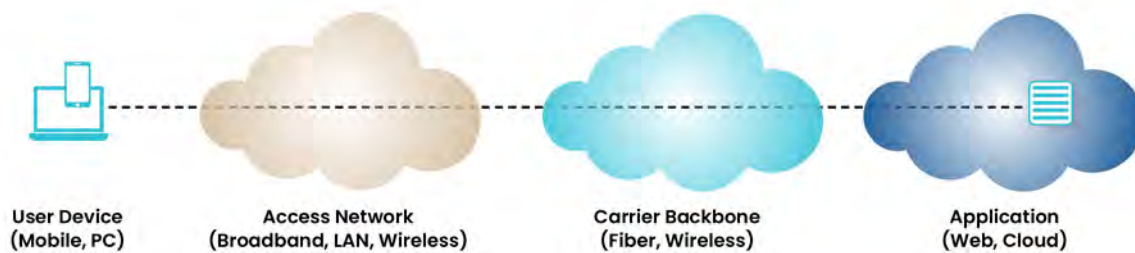
**Key Point:** The value proposition for small business customers must focus on addressing threat concerns, maintaining low cost and requiring zero effort from the business.

## 6.2 Telecom Options to Provide Security to Home and Small Business Customers

Telecoms have multiple means to support home, small business and microbusiness security needs. This starts with resource options such as online sites with FAQs,<sup>73</sup> forums, and even support for social channels that allow customers to ask each other questions about security.<sup>74</sup> Additionally, telecoms can simply resell security products or services through their existing channels, including retail centers. Mobile security apps, for example, have been resold by telecoms frequently—usually with low levels of success.<sup>75</sup>

Accordingly, to provide effective functional support for cybersecurity, telecoms have the option to integrate their protections into the end-to-end infrastructure supporting their customer's use of the internet. Such use can be modeled by the device-to-app setup so common for home, small business and microbusiness customers. This device-to-app use case can include the telecom in the network path, but when customers use their device in a café, airport, neighbor's home or other location, the use case might involve another telecom's service infrastructure.

In every possible use case arrangement, the end user is in possession of a device that uses some sort of local network or internet access to establish a connection with a desired application or service. This can include email, websites, games or hosted applications in support of some personal or business activity. It is also worth mentioning that such access will in many cases involve intentional access to content that might not traditionally be associated with social or business value (e.g., gambling, adult). By some estimates, 35 percent of all internet downloads involve adult content.<sup>76</sup>



**Figure 6.2-1. Device-to-App Use Case View**

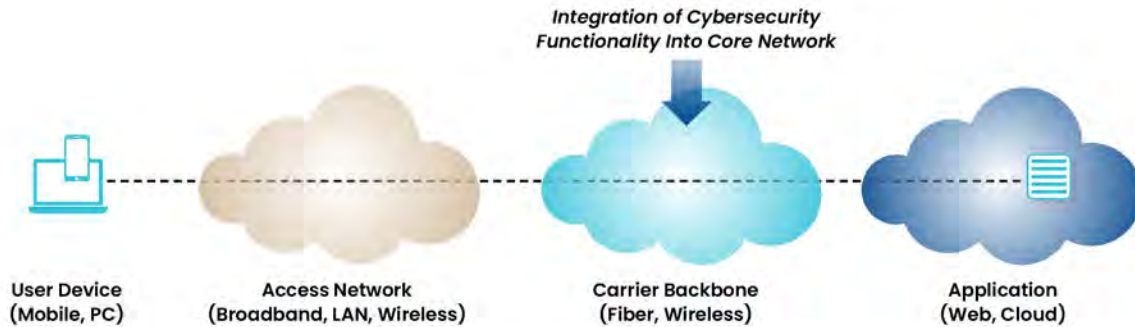
The device-to-app view offers insights into the opportunities that telecoms have to embed security controls into the access path. This includes the user device (endpoint), local access path (premise) and carrier backbone (code network). These are the best options for integrating security into the path used by families and small business users to access the applications that they need from the web or cloud.

While telecoms can certainly engage with cloud infrastructure to help protect hosted applications, it can be assumed that this work would be highly integrated with the cloud service provider, to the degree that this becomes a separate business activity, such as peering services between telecom backbones and major cloud services.<sup>77</sup> This is considered outside the scope of this report, since telecom business relationships with cloud providers is neither home- nor small business-oriented.

### 6.2.1 Core Network Security

The core network backbone for telecom carriers includes three broad types of infrastructure: (1) wireless infrastructure, including radio access network (RAN) services; (2) fiber infrastructure deployed from the broadband edge to the high-speed core; and (3) network management systems, which include a massively wide range of control, administration, maintenance, billing, security, diagnostic and other services.

These core network components represent options for the integration of additional security services for home and small business customers. For this to be done, the telecom would have to include the means to identify these users through some designation (e.g., identity, IP address, account information) and then route the connection toward the additional security if appropriate (e.g., user directly paying for the service, user part of a group paying for the service).

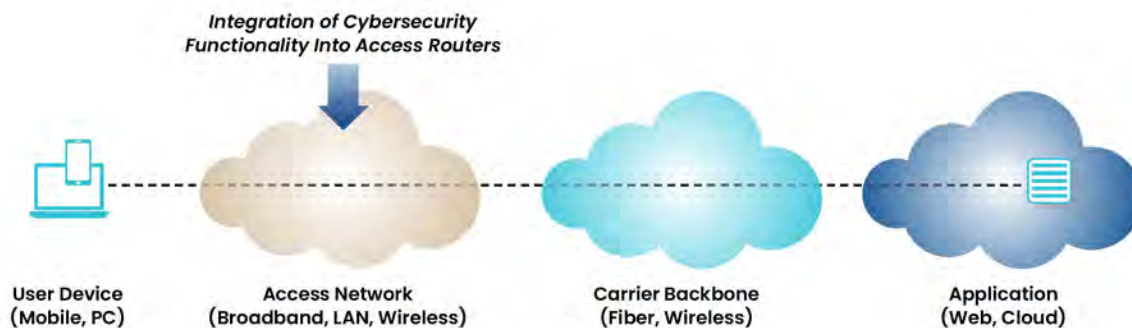


**Figure 6.2.1-1. Core Network Options for Home and Small Business Security**

### 6.2.2 Premise Router Security

The premise network infrastructure for the home and small business will include a diverse assortment of options, especially for businesses that include a physical, shared office for employees, perhaps in a landlord-supported building, versus all employees working virtually from their homes. In all cases, the access begins with a Wi-Fi connection, a 3G/4G/5G wireless connection or a direct Ethernet connection.<sup>78</sup>

A good premise option for telecoms to integrate security involves the router that is deployed to the home or small business. The router is a convenient aggregation point for both Wi-Fi and broadband access, but it does not account for direct 3G/4G/5G wireless access services that might cover the local premise. This implies that users will have two paths to access applications: (1) premise router access via Wi-Fi or Ethernet; or (2) wireless access via the carrier 3G/4G/5G signal.

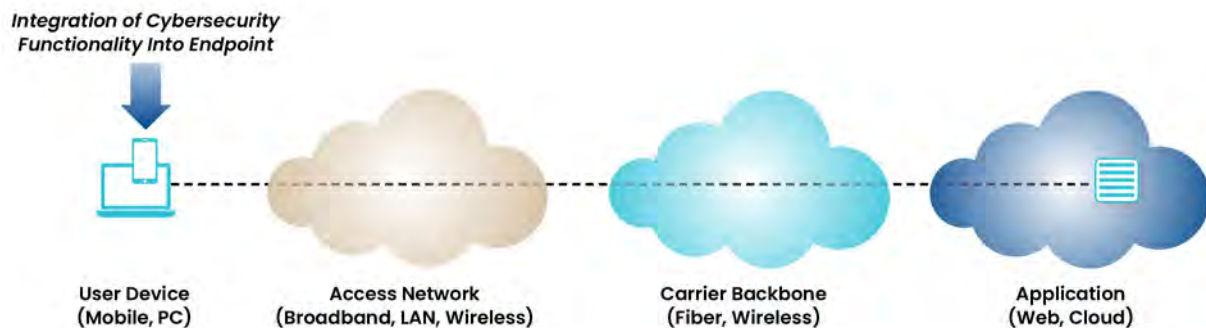


**Figure 6.2.2-1. Premise Router Options for Home and Small Business Security**

### 6.2.3 Endpoint Security

The endpoint devices in a home or small business include primarily PCs, tablets and mobile devices. Additional internet of things (IoT) devices found primarily in the home include gaming consoles, smart TVs, smart printers, voice-controlled virtual assistants and other types of connected systems. All of these can be considered endpoints, but the primary use case for access involves the Windows or Mac PC, and the mobile tablet or handset (Apple or Android).<sup>79</sup>

The best endpoint option for telecoms to integrate security involves targeting the PCs and mobile devices, because these are the main access devices that family members and small business employees use on a day-to-day basis to connect to apps and websites. This implies that additional security controls from the carrier can be introduced to the PC or mobile, perhaps through resale of an existing antimalware solution.



**Figure 6.2.3-1. Endpoint Options for Home and Small Business Security**

### 6.3 Go-to-Market Plan

Telecoms that choose to select one or more of the options presented above for offering enhanced security to home users and small businesses must create a go-to-market strategy that supports practical considerations such as selecting a suitable commercial partner, testing, and implementing the platform in the production network, and then working together to create a service value proposition for customers.

One case study worth reviewing is the provision of PC Matic security software for the home and small business.<sup>80</sup> The company reaches and communicates with home users and small businesses through extensive spend on television commercials.<sup>81</sup> Despite the somewhat dubious value of the PC software,<sup>82</sup> PC Matic has succeeded by reaching out directly and aggressively to the home and small business customer.

The details of a go-to-market plan are beyond the scope of this report, but this research was performed in conjunction with the team from Allot Ltd. The next section illustrates how a telecom might go about integrating Allot’s capabilities, which track closely with the features presented above. As such, the Allot use case is both a practical option that can be implemented immediately and a validation of the overall concept.

## 7. OVERVIEW OF THE ALLOT PLATFORM

Founded in 1996 and listed on Nasdaq (ALLT) and the TASE (ALLT), Allot Ltd. is a technology firm headquartered in Israel that provides advanced telecom solutions, including a wide range of cybersecurity solutions for home users and businesses. The company has supported over 3,000 installations serving 1 billion users through service provider customers in over 100 countries.<sup>83</sup>

### 7.1 Allot Customer Base

Allot has worked extensively with ISPs and mobile network operators and has provided excellent guidance on go-to-market strategies for these customers, including resources on how to roll out SaaS in conjunction with the Allot team.<sup>84</sup> Current global telecommunications service provider customers of Allot’s technology include the following companies:<sup>85</sup>

**7.1.1 Telefonica**—Since 2020,<sup>86</sup> Allot has powered the Telefonica Conexion Segura SECaaS service in Spain

to protect small and midsize businesses from cyberthreats. The offer includes McAfee MultiAccess<sup>87</sup> to ensure privacy control for up to 10 SMB devices. The Telefonica solution leverages the Allot NetworkSecure<sup>88</sup> solution to address ransomware, malicious third-party sites and malware in fixed and mobile networks. Revenue is shared between Telefonica, Allot and McAfee. The Telefonica solution, which is installed at the core of its network, includes URL protection against risky or content-inappropriate sites.

**7.1.2 DISH**—DISH Network Corporation announced in April 2021 that it would deploy the Allot platform to provide User Plane Protection (UPP)<sup>89</sup> against DDoS and botnet attacks on its OpenRAN-based 5G network.<sup>90</sup> DISH is also partnering with Allot to provide security services for MVNO and SMB customers.

**7.1.3 Safaricom**—Kenya-based Safaricom<sup>91</sup> announced in 2019 that it would partner with Allot on a combined DDoS Secure<sup>92</sup> and NetworkSecure solution designed to provide network analytics, network security and protections against DDoS.<sup>93</sup>

**7.1.4 Rakuten**—Japanese mobile network provider Rakuten announced in 2019 that it would leverage Allot’s network-based traffic management system and security solutions to deliver a fully secure mobile network that protects Rakuten’s mobile network and subscriber traffic.<sup>94</sup>

**7.1.5 Exetel**—Australian ISP Exetel announced in 2021 that it would utilize the Allot NetworkSecure platform to secure services and provide parental content controls.<sup>95</sup>

**7.1.6 Eolo**—Italian fixed wireless broadband provider Eolo announced in 2021 an expansion of its contract with Allot to provide expanded security services to its customers.<sup>96</sup>

**7.1.7 Vodafone**—Since 2015, Vodafone Germany has offered a Secure Net solution as an add-on offering based on the Allot platform. The solution was designed to integrate the Allot Service Gateway<sup>97</sup> and Allot WebSafe Personal into a SECaaS.<sup>99</sup>

## 7.2 Allot Services Overview

The services offered by Allot to its customers can be grouped into five main offers: HomeSecure, EndpointSecure, NetworkSecure, IoTSecure and DDoS Secure. These solutions are all designed to support high adoption rates for ISPs and to increase brand loyalty for the ISP through the addition of security protection for its own end users. The financial goal is to increase average revenue per user (ARPU)<sup>100</sup> for ISPs.<sup>101</sup>

The architecture of the various Allot services can be visualized in a diagram that the company provides on its website and in various presentations (see Figure 7.2-1).

### 7.2.1 HomeSecure

Allot HomeSecure<sup>103</sup> provides security for IoT, smart appliances and home offices. The service adds a thin client to existing customer premise equipment (CPE) to provide home network visibility and protections. This service involves installation of a

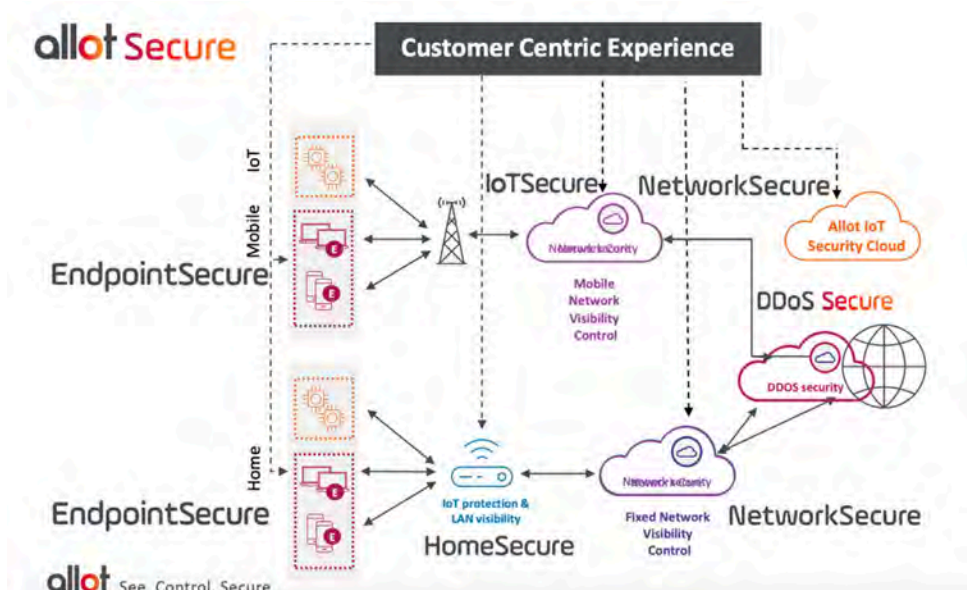


Figure 7.2-1. Allot Service Architecture

security agent onto existing CPE router equipment that connects to the Allot Secure Cloud.

Security advantages of HomeSecure include (1) protection of all devices within the home through identification and subjected to a tailored security policy; (2) protection of the home network (intradevice attack within the home); and (3) protection of the CPE router itself, including password strength enforcement, open port analysis and access controls to prevent unauthorized access.<sup>104</sup>

### *7.2.2 EndpointSecure*

Allot EndpointSecure<sup>105</sup> leverages the Bitdefender technology<sup>106</sup> to provide protection and content filtering for consumers and small business users. Since this solution involves an endpoint security agent, it provides persistent protection of the device, even when the user travels away from the home network. This includes content filtering for children who might bring their device to school or other family homes.

Security advantages of EndpointSecure include (1) threat protection for devices from access to malicious websites; (2) category-based content filtering of websites, including parental controls for quiet time and application blocking; (3) antitheft and location management, including a map that shows the current geographic position of the device; and (4) integration with the AllotSecure platform for reporting.

### *7.2.3 NetworkSecure*

Allot NetworkSecure<sup>107</sup> delivers personalized security and parental controls that are automatically provided to mass market customer bases from within the ISP core network. This involves zero touch for the customer, with frictionless onboarding, because the technology is embedded into the service provider infrastructure. Deployment is done as a virtual network function (VNF),<sup>108</sup> through stand-alone software or hosted on the Allot Service Gateway.

Security advantages of NetworkSecure include (1) security for users of mobile networks who require security protection but who might prefer to not run a client-based solution; (2) multitenant architecture, so that large numbers of customers can be protected; and (3) security support for both fixed access and radio access over the service provider's fiber/broadband and wireless networks.

### *7.2.4 IoTSecure*

Allot IoTSecure<sup>109</sup> is designed to protect IoT connectivity for mobile IoT devices. Without sufficient IoT protections, vulnerable devices can connect to botnets and other threats. They can also become barraged with unsolicited traffic from web crawlers and other bots. This can degrade or drain battery life, consume end user data plans, and create significant issues with the service provider regarding billing.

Security advantages of IoTSecure include (1) protection of IoT customers from rogue devices being inserted into the network; (2) enforcement of access controls; (3) network-based security that inspects downloads for IoT malware; (4) behavioral profiling to identify misbehaving devices; (5) alerting on detection of issues; and (6) support for DDoS threats to IoT infrastructure.

### *7.2.5 DDoS Secure*

Allot DDoS Secure<sup>110</sup> is designed to offer full distributed DDoS protection and bot containment for communication service provider networks. The Allot solution offers mobile, fixed and cloud service providers with DDoS security against layer 3 volumetric attacks, and to neutralize outbound threats before they can introduce performance degradation into network services.

Security advantages of DDoS Secure include (1) reduction of business risk and downtime to assure quality of experience (QoE); (2) real-time inline detection and blocking; (3) bidirectional support from

within the ISP infrastructure; and (4) Allot Service Gateway deployment via a blade appliance (sensor) and central management controller with automatic attack mitigation capabilities.<sup>11</sup>

### 7.2.6 DNS Secure

Allot DNS Secure<sup>12</sup> offers network-based security, including threat protection and parental control functions for consumers. The goal of using the Domain Name System (DNS)<sup>13</sup> as the basis for security is to offer protections to complement client-based solutions (which might not have been deployed or used) and to provide a more transparent type of security and content filtering.

Security advantages of DNS Secure include (1) a threat database for antimalware, antiphishing, botnet avoidance and adware security; (2) URL and virus protection through scanning of covered traffic selected and sent to the Allot DNS Secure proxy; and (3) domain reputation-based category filtering, with multiple categories available to manage and monitor web browsing and application usage.

### 7.2.7 BusinessSecure

Allot BusinessSecure<sup>14</sup> offers network security for small and midsize businesses. The goal is to block external and internal attacks through advanced security and network visibility. The service is designed to address potentially growing SMB networks, including ones that must support bring your own device (BYOD)<sup>15</sup> policies, in which employees might be bringing infected devices to the office network.

Security advantages of BusinessSecure include (1) protection of the SMB CPE router from security vulnerabilities through deployment of an agent; (2) visibility into the end user, including support for iOS and Android; (3) security policy control for SMB networks, including time of day limitations; and (4) protection of mobile, work and off-net devices with content controls and security.

### 7.2.8 5G NetProtect

Allot 5G NetProtect<sup>16</sup> is designed to protect the 5G network to ensure optimal QoE for all service delivered across carrier wireless infrastructure. Such security is essential to protect infrastructure being connected to 5G wireless services, including telehealth, autonomous cars and many other applications. The service includes support for deep packet inspection (DPI)-based policy controls embedded into the 5G core.

Security advantages of 5G NetProtect include (1) reduction in network downtime by blocking known and unknown threats; (2) avoidance of brand and reputation impacts by stopping weaponized IoT and botnet attacks; and (3) support via cloud-native solutions designed for 5G providers that secure the user plane by insertion into the 5G interface that delivers customer traffic into the core.

## 8. SAMPLE BUSINESS CASE FOR TELECOM SERVICE PROVIDERS

Telecom service providers, especially in the U.S., are well-positioned in 2022 and beyond to move forward with the Allot suite of advanced cybersecurity controls for families and small businesses. With the obvious proliferation and growth of malicious threats, smaller customers of ISP services are likely more willing than ever to consume and use these services from their ISPs, as long as the pricing is reasonable and the administration minimal.

In this section, we introduce a sample step-by-step business case for a hypothetical telecom service provider, ACME Telecom, to expand its offerings, infrastructure controls and resold products into a coherent and uniform new offering, based on the Allot security solutions. This offering can increase ARPU, reduce security threats (to end users as well as the ISP infrastructure) and improve customer satisfaction with their ISP experience.<sup>17</sup>

This section assumes that ACME Telecom will make direct use of the Allot platform<sup>18</sup> and the services described above. This research report from TAG Cyber makes the case that the Allot solution is well-

positioned to offer the type of service support required to accomplish the goals just listed. Tag Cyber, with its years of experience and market analysis, is unaware of any competing platform that offers comparable benefit and coverage.<sup>119</sup>

### *8.1 Sample Business Case Development*

The ACME Telecom business case has the following goal: to demonstrate that the Allot platform can be integrated into the service infrastructure to create meaningful financial returns and improve the customer Net Promoter Score (NPS).<sup>120</sup> The assumption is that the current NPS score is a neutral 6 and that ACME Telecom would like to move into the 7/8 passive or even the 9/10 promoter categories.

It will be assumed that ACME Telecom is planning two new service offerings for its broadband customers. The first will be called ACME Protect and will include security in the core and CPE router. The second will be called ACME Protect Plus and will include security in the core, CPE router and endpoint. In this sample case, it is assumed (to simplify the discussion) that plans will be made later to include security options for ACME Telecom wireless customers.

### *8.2 Sample Revenue Estimates*

It is assumed that ACME Telecom has a business case process in place that supports development of revenue estimates.<sup>121</sup> One quantitative finding regarding the ACME Telecom customer base of 10 million home broadband customers (reached via fiber) and 5,000 business customers (reached in their business locations) is that 60 percent of families and businesses expressed strong interest in these service options, according to a direct survey.<sup>122</sup>

From a baseline perspective, subscriber estimates imply that ACME Telecom is a roughly \$12 billion company. This is much smaller than Verizon, which reported \$128 billion in revenue in 2020,<sup>123</sup> and much smaller than AT&T, which reported \$170 billion in revenue in 2020. Most U.S. telecom companies will report annual revenue considerably lower than that of Verizon and AT&T, hence the lower assumptions for ACME Telecom in this study.

Using models, ACME Telecom determines that ACME Protect will see a 50 percent take and ACME ProtectPlus will see an additional 10 percent take for families and SMBs at a 5 percent and 6 percent increase to existing monthly service fees, respectively. Since existing ARPU for families is \$100 per month, and existing ARPU for SMBs is also \$200 per month, this represents an increased monthly fee of \$5 and \$10 per month for families and businesses, respectively, for ACME Protect.<sup>124</sup>

Doing the math, this represents an increase in annual revenue for both services of \$309 million, which represents roughly a 2.5 percent increase in total revenue for ACME Telecom. This type of increase can have positive implications for the valuation of a company for investors, but this improved total value is not factored into the business case estimation presented in this report (since Wall Street valuations can be so unpredictable).

It is also worth noting that the revenue estimates made in this section are for a steady-state target in which all promotion and marketing work is in full throttle, and all achievable sales targets have been reached. This is an important consideration, because the ROI calculation over five years (see below) will include a gradual ramp-up to the full-throttle revenue targets for all security services.



	Annual Existing ARPU	Added Annual ARPU From ACME Protect	Added Annual ARPU With ACME Protect Plus	Annual New Revenue (ACME Protect) at 50% Take	Total New Revenue for Security	Total New Revenue for Security
Family Subscribers	\$1200/yr	\$60/yr	\$12/yr	\$300.00M	\$6.00M	\$306.00M
SMB Subscribers	\$240/yr	\$120/yr	\$24/yr	\$3.00M	\$0.06M	\$3.06M
<b>Total</b>				<b>\$303.00M</b>	<b>\$6.06M</b>	<b>\$309.06M</b>

**Revenue Case Assumptions**

- Total Family Subscribers = 10M
- Total SMB Subscribers = 50,000
- Total ACME Protect Take Rate – 50% = 5,025,000 customers
- Total ACME Protect Plus Take Rate – Additional 10%
- Additional New Revenue for ACME Protect: \$60 per year at 5M family customers
- Additional New Revenue for ACME Protect: \$120 per year at 25,000 SMB customers
- Additional New Revenue for ACME Protect: Plus: \$12 per year at 500,000 family customers
- Additional New Revenue for ACME Protect: Plus: \$24 per year at 2,500 SMB customers

**Figure 8.2–1. Steady-State Revenue Estimates for ACME Protect and ACME Protect Plus**

**8.3 Sample Cost Estimates**

The corresponding cost estimates for the ACME Protect and ACME Protect Plus offerings assume five categories of costs: (1) revenue share (license) fees paid to Allot for use of the platform and solutions;<sup>125</sup> (2) engineering and installation costs;<sup>126</sup> (3) ongoing support and maintenance costs; (4) customer care and support costs, plus training; and (5) sales and marketing expenses.

While license fees will vary according to negotiated deals, we will assume here that the ISP has negotiated a revenue share deal in which Allot will receive a percentage of all new revenue, based on the security services offered.<sup>127</sup> The percentage is likely to be negotiated on a graduated basis with Allot so that fees for the ISP will increase or decrease as the revenue increases above some designated threshold.

Other estimated costs for this hypothetical case are based on the experience of the TAG Cyber analysts with this type of work activities in a typical telecom environment.<sup>128</sup> Costs for engineering and installation, support and maintenance, customer care, and sales and marketing are provided at steady-state levels. These costs might start higher or lower, and ramp up to steady-state. A sample such effect is included in the ROI calculation in the next section.

	40% Revenue Share Costs to Allot (Ongoing)	Engineering and Installation Costs (One-Time)	Support and Maintenance Costs (Ongoing)	Care and Support Costs Plus Training (Ongoing)	Sales and Marketing Costs (Ongoing)	Total New Costs for Security
Expense	\$120M	\$5M	\$5Mr	\$20M	\$20M	\$165M
Capital	N/A	\$2M	\$1M	N/A	N/A	\$1M
<b>Total</b>	<b>\$120M</b>	<b>\$7M</b>	<b>\$6M</b>	<b>\$20M</b>	<b>\$20M</b>	<b>\$166M</b>

**Revenue Case Assumptions**

- The costs listed here are for steady-state. Costs will vary during early and later stages of deployment.
- Revenue share costs are based on \$300M for family subscribers and \$3M for SMB subscribers.
- Expense versus capital determinations will vary according to local CFO policy.
- Capital costs are relevant to network and CPE hardware and associated maintenance.
- Revenue share of 40% assumes that Allot shares payment with Bitdefender for ACME Protect Plus.
- Engineering and installation costs are included but will decrease after 1 year of deployment—not included in Total New Costs (recurring).
- Total costs combine expense and capital for illustration. Most CFO teams will track separately.
- Capital costs here do not include the positive effect of multiyear capital accounting schedules.
- The \$20M Sales and Marketing expense include advertising (e.g., TV) to drive the 50% targeted take rates for families and SMB.

**Figure 8.3–1. Steady-State Cost Estimates for ACME Protect and ACME Protect Plus**

#### 8.4 Sample Income Statement

To calculate the income and investment returns for the ACME Protect and ACME Protect Plus service offerings, we present below a five-year view with a graduated sales take rate that assume five years to reach the targeted sales volumes, followed by steady continued sales at the targeted and assumed rates of sales. We also assume that the largest one-time engineering fees, training costs and marketing expenses are completed in the first two years.

The income statement is developed with the reasonable view that to obtain out-year returns that include significant income to the telecom (e.g., \$134 million operating income in year five is based on the sample analysis and assumptions), some investment is required in year one, including a break-even return based on early sales estimates and higher engineering and installation costs for the network and CPE portions of the project.

The operating income estimates also do not consider the effect of tax, depreciation and other costs related to capital or other details. Nevertheless, the returns on this investment for ACME regarding ACME Protect and ACME Protect Plus are considerable. Also, if sales are not reaching the expected volumes, then it will be straightforward to steer down expenses using a revenue share approach, especially since license fees are the highest cost in most years.

**ACME Protect and Protect Plus Consolidated Income Statement of Operations**  
(in USD \$ millions)

	Year 1	Year 2	Year 3	Year 4	Year 5
<b>Revenue</b>	80	120	180	250	300
<b>Net Sales</b>	80	120	180	250	300
<b>Costs of Revenue</b>	80	81	113	141	1666
<b>License Fees</b>	32	48	72	100	120
<b>Engineering</b>	7	2	0	0	0
<b>Maintenance</b>	6	6	6	6	6
<b>Customer Care</b>	15	15	15	15	20
<b>Marketing</b>	20	20	20	20	20
<b>Operating Income</b>	(0)	39	67	109	134

**Figure 8.4-1. Five-Year Income Statement Estimate for ACME Protect and ACME Protect Plus**

## Footnotes

- <sup>1</sup> The research and recommendations offered in this note were developed in conjunction with the team at Allot Ltd. The goal was to identify security challenges for home and small business and microbusiness users in the U.S. market and to develop recommendations for how service providers can take advantage of this opportunity. Information on Allot can be obtained at <https://www.allot.com/>.
- <sup>2</sup> [https://en.wikipedia.org/wiki/Antivirus\\_software](https://en.wikipedia.org/wiki/Antivirus_software)
- <sup>3</sup> Emphasis in this report is on the domestic telecommunications infrastructure in the United States. All concepts presented here are applicable to most international environments, but some countries include unique requirements driven by local government. The discussions in this report thus presume U.S. infrastructure unless otherwise designated.
- <sup>4</sup> <https://www.techradar.com/vpn/how-to-set-up-and-use-a-vpn-to-help-you-work-from-home>
- <sup>5</sup> <https://www.verizon.com/solutions-and-services/content-filters/>
- <sup>6</sup> <https://www.xfinity.com/support/articles/xfinity-xfi-overview>
- <sup>7</sup> <https://www.commonsemmedia.org/blog/parents-ultimate-guide-to-parental-controls>
- <sup>8</sup> <https://www.malwarebytes.com/>
- <sup>9</sup> <https://www.digitaltrends.com/computing/does-your-mac-need-antivirus/>
- <sup>10</sup> <https://www.usnews.com/360-reviews/antivirus/how-does-antivirus-software-work>
- <sup>11</sup> <https://www.avg.com/en/signal/remove-phone-virus#gref>
- <sup>12</sup> <https://www.techradar.com/news/using-an-iphone-may-not-be-as-safe-as-you-thought>
- <sup>13</sup> <https://www.avg.com/en/signal/remove-phone-virus#gref>
- <sup>14</sup> <https://www.t-mobile.com/brand/data-breach-2021>
- <sup>15</sup> <https://www.usnews.com/360-reviews/identity-theft-protection>
- <sup>16</sup> <https://www.consumer.ftc.gov/articles/how-avoid-scam>
- <sup>17</sup> <https://www.pcmag.com/picks/the-best-password-managers>
- <sup>18</sup> <https://www.wired.com/story/netflix-password-sharing-crackdown/>
- <sup>19</sup> <https://www.washingtonpost.com/technology/2021/09/29/hacked-social-media-account/>
- <sup>20</sup> <https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats>
- <sup>21</sup> <https://www.visa.com/splisting/searchGrsp.do>
- <sup>22</sup> <https://www.aadyasecurity.com/news/5-things-all-small-businesses-should-be-doing-to-protect-client-data/>
- <sup>23</sup> <https://www.americanexpress.com/en-us/business/trends-and-insights/articles/7-ways-to-help-keep-your-customer-data-safe-as-home-based-business/>
- <sup>24</sup> <https://gusto.com/security>
- <sup>25</sup> <https://www.mimecast.com/blog/why-online-brand-protection-is-important-for-small-businesses/>
- <sup>26</sup> <https://www.business.com/articles/tips-prevent-brand-fraud/>
- <sup>27</sup> <https://securityscorecard.com/blog/what-can-cybersecurity-ratings-do-for-service-providers>
- <sup>28</sup> <https://www.cybergix.com/>
- <sup>29</sup> <https://www.wework.com/legal/global-privacy-policy>
- <sup>30</sup> <https://www.darkreading.com/risk/wework-s-wi-fi-exposed-files-credentials-emails>
- <sup>31</sup> <https://www.consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network>
- <sup>32</sup> <https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-saas.html>
- <sup>33</sup> <https://sirix.tech/>
- <sup>34</sup> [https://play.google.com/store/apps/details?id=com.google.android.authenticator2&hl=en\\_US&gl=US](https://play.google.com/store/apps/details?id=com.google.android.authenticator2&hl=en_US&gl=US)
- <sup>35</sup> <https://www.ericsson.com/en/network-slicing/ran-slicing>
- <sup>36</sup> <https://www.techradar.com/news/fewer-americans-trust-isps-to-look-out-for-their-best-interests>
- <sup>37</sup> <https://about.att.com/story/2021/robocalls.html>
- <sup>38</sup> <https://about.att.com/pages/cyberaware/ae/fraud>
- <sup>39</sup> [https://www.usenix.org/legacy/event/sruti05/tech/full\\_papers/xu/xu.pdf](https://www.usenix.org/legacy/event/sruti05/tech/full_papers/xu/xu.pdf)
- <sup>40</sup> <https://help.campaignmonitor.com/how-why-isps-block-emails>
- <sup>41</sup> <https://thoughtthatcounts.economist.com/planning-tools/rate-cards#the-economist>
- <sup>42</sup> <https://www.sciencedaily.com/releases/2020/08/200812115248.htm>
- <sup>43</sup> <https://www.verizon.com/business/support/fios-internet/wireless-network-encryption-faqs/>
- <sup>44</sup> <https://www.silentcircle.com/>
- <sup>45</sup> <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/>
- <sup>46</sup> [https://www.researchgate.net/publication/226690941\\_Network\\_Security\\_-\\_A\\_Service\\_Provider\\_View](https://www.researchgate.net/publication/226690941_Network_Security_-_A_Service_Provider_View)
- <sup>47</sup> <https://www.wired.com/story/google-internet-traffic-china-russia-rerouted/>
- <sup>48</sup> <https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance>
- <sup>49</sup> <https://arstechnica.com/information-technology/2015/03/atts-plan-to-watch-your-web-browsing-and-what-you-can-do-about-it/3/>
- <sup>50</sup> [https://en.wikipedia.org/wiki/Hepting\\_v.\\_AT%26T](https://en.wikipedia.org/wiki/Hepting_v._AT%26T)
- <sup>51</sup> <https://www.fastcompany.com/90421616/heres-how-to-stop-comcast-verizon-and-other-isps-from-spying-on-you>
- <sup>52</sup> <https://www.forbes.com/sites/forbestechcouncil/2021/04/15/edr-xdr-and-mdr-understanding-the-differences-behind-the-acronyms/?sh=27c6b04449e2>
- <sup>53</sup> <https://www.verizon.com/business/resources/reports/dbir/>
- <sup>54</sup> <https://www.g2.com/categories/secure-web-gateways/small-business>
- <sup>55</sup> <https://cloudsmallbusinessservice.com/blog/top-10-cloud-based-web-content-filtering-software-for-business-68592.html>
- <sup>56</sup> <https://edtechmagazine.com/kt2/article/2019/04/how-k-12-schools-can-use-next-generation-content-filtering-keep-students-safe-perfcon>
- <sup>57</sup> <https://business.comcast.com/learn/internet/security-edge>
- <sup>58</sup> <https://enterprise.verizon.com/resources/articles/ddos-protection-service-ddos-shield/>
- <sup>59</sup> <https://www.godaddy.com/web-security/website-security>
- <sup>60</sup> <https://www.pcmag.com/news/how-to-secure-your-e-commerce-website-6-basic-steps>
- <sup>61</sup> <https://www.pcmag.com/reviews/logicmonitor>
- <sup>62</sup> <https://www.centurylink.com/small-business/CLEC/ManagedServices/managedSecurity.vm>
- <sup>63</sup> <https://www.huntress.com/>
- <sup>64</sup> <https://www.centurylink.com/small-business/CLEC/ManagedServices/managedSecurity.vm>
- <sup>65</sup> <https://www.apple.com/retail/geniusbar/>
- <sup>66</sup> New Jersey-based navitend is a typical MSP that offers small business support to the local community. <https://www.navitend.com/>
- <sup>67</sup> [https://en.wikipedia.org/wiki/Geek\\_Squad](https://en.wikipedia.org/wiki/Geek_Squad)
- <sup>68</sup> <https://www.cnn.com/2021/08/10/main-street-overconfidence-small-businesses-dont-worry-about-hacking.html>
- <sup>69</sup> <https://www.lightreading.com/security/t-mobile-to-join-atandt-verizon-in-selling-customers-data/d/d-id/767955>
- <sup>70</sup> <https://www.pewresearch.org/internet/2011/03/17/attitudes-towards-the-internets-impact-on-politics/>
- <sup>71</sup> <https://vrkascpas.com/the-4-quickbooks-reports-small-business-owners-need/>
- <sup>72</sup> <https://quickbooks.intuit.com/ca/resources/business/whats-the-difference-micro-and-small-businesses/>
- <sup>73</sup> <https://www.verizon.com/business/products/security/>
- <sup>74</sup> <https://www.zendesk.com/blog/customer-service-through-social-media/>
- <sup>75</sup> <https://medium.com/chip-monks/at-t-to-install-lookout-security-app-on-all-android-phones-2de65ab0706e>
- <sup>76</sup> <https://www.webroot.com/us/en/resources/tips-articles/internet-pornography-by-the-numbers>
- <sup>77</sup> <https://www.business.att.com/products/netbond.html>
- <sup>78</sup> <https://www.sciencedirect.com/science/article/pii/S030859612100032X>
- <sup>79</sup> As referenced earlier, many home users rely on a company-issued PC and/or mobile as their primary device(s).
- <sup>80</sup> <https://www.pcmatic.com/>
- <sup>81</sup> <https://www.pcmatic.com/company/commercials.asp>
- <sup>82</sup> <https://www.pccomputerguy.com/Tech-Tips-Article-Pc-Matic>
- <sup>83</sup> This report from TAG Cyber represents research sponsored by Allot to identify the best means for marketing, integrating, and supporting telecom and ISP provision of home and small/micro business security services in the US market circa early 2022 and beyond.
- <sup>84</sup> [https://www.allot.com/resources/066\\_MobileTrends\\_Dec\\_2017\\_C\\_WEB.pdf](https://www.allot.com/resources/066_MobileTrends_Dec_2017_C_WEB.pdf)
- <sup>85</sup> This section lists and includes several prominent ISP or mobile service provider customers of Allot for which a public press release or article is available on the Internet. Enterprise customers are not listed, and many other ISP customers are obviously omitted here. The goal is to just offer a sampling of typical recent engagements.
- <sup>86</sup> <https://www.allot.com/corporate/media-center/press-releases/telefonica-expends-security-as-service-protecting-spanish-smb-against-cyberattacks/>
- <sup>87</sup> <https://www.costco.com/wcsstore/CostcoUSBCatalogAssetStore/Attachment/mma-costco-flyer-151205.pdf>
- <sup>88</sup> Allot NetworkSecure provides URL filtering controls. <https://www.allot.com/products-service-providers/network-security-services/>
- <sup>89</sup> <https://www.metaspitch.com/knowledge-center/reference/what-is-the-5g-user-plane-function-upf>
- <sup>90</sup> <https://www.allot.com/corporate/media-center/press-releases/dish-selects-allot-to-protect-5g-network/>
- <sup>91</sup> <https://www.safaricom.co.ke/personal/>
- <sup>92</sup> Allot DDoS Secure provides protection against DDoS attacks. <https://www.allot.com/service-providers/ddos-protection/>
- <sup>93</sup> [https://www.securityinformed.com/news/allot-communications-implement-convergent-network-solution-co-14424-ga1550060874.html?utm\\_source=SSC%20International%20Edition&utm\\_medium=Redirect&utm\\_campaign=International%20Redirect%20Popup](https://www.securityinformed.com/news/allot-communications-implement-convergent-network-solution-co-14424-ga1550060874.html?utm_source=SSC%20International%20Edition&utm_medium=Redirect&utm_campaign=International%20Redirect%20Popup)

- <sup>94</sup> <https://www.allot.com/corporate/media-center/press-releases/allot-to-partner-with-rakuten-mobile/>
- <sup>95</sup> <https://www.allot.com/corporate/media-center/press-releases/exetel-launches-anti-malware-parental-control/>
- <sup>96</sup> <https://www.telecompaper.com/news/italys-eolo-expands-allot-security-contract--1398128>
- <sup>97</sup> <https://www.telcotitans.com/vodafonewatch/allot-reports-continual-growth-for-uptake-of-vodafone-secure-net/881.article>
- <sup>98</sup> <https://www.allot.com/products-enterprise/service-gateway/>
- <sup>99</sup> <https://www.allot.com/corporate/media-center/press-releases/vodafone-germany-makes-web-surfing-secure-with-allot-websafe-personal/>
- <sup>100</sup> [https://en.wikipedia.org/wiki/Average\\_revenue\\_per\\_user#:~:text=In%20mobile%20telephony%2C%20ARPU%20includes,within%20the%20regulatory%20interconnection%20regime.](https://en.wikipedia.org/wiki/Average_revenue_per_user#:~:text=In%20mobile%20telephony%2C%20ARPU%20includes,within%20the%20regulatory%20interconnection%20regime.)
- <sup>101</sup> Hutchison Dre Austria claims to have increased their ARPU based on a deployment of the Allot platform. <https://www.allot.com/resources/success-stories/hutchison-dre-austria/>
- <sup>102</sup> <https://investors.allot.com/static-files/25e89b89-d745-4001-8926-d4eac8e2c6b8>
- <sup>103</sup> [https://www.allot.com/resources/BR\\_Allot-HomeSecure\\_web2.pdf](https://www.allot.com/resources/BR_Allot-HomeSecure_web2.pdf)
- <sup>104</sup> An excellent white paper is available from Patrick Donegan of HardenStance that lays out the risks that have emerged to home routers and how solutions such as Allot's can help to reduce this risk. <https://www.allot.com/cyberhub/home-router-security-the-buck-stops-where-a-hardenstance-whitepaper/>
- <sup>105</sup> [https://www.allot.com/resources/DS\\_EndpointSecure.pdf](https://www.allot.com/resources/DS_EndpointSecure.pdf)
- <sup>106</sup> <https://www.bitdefender.com/support/bitdefender-endpoint-security.html>
- <sup>107</sup> <https://www.allot.com/resources/DS-NetworkSecure.pdf>
- <sup>108</sup> <https://www.techtarget.com/searchnetworking/definition/virtual-network-functions-VNF>
- <sup>109</sup> <https://www.allot.com/service-providers/iot-security-solutions/>
- <sup>110</sup> <https://www.allot.com/products-service-providers/ddos-security/>
- <sup>111</sup> [https://www.allot.com/resources/DS\\_DDoS-Secure.pdf](https://www.allot.com/resources/DS_DDoS-Secure.pdf)
- <sup>112</sup> <https://www.allot.com/products-service-providers/dns-secure/>
- <sup>113</sup> [https://en.wikipedia.org/wiki/Domain\\_Name\\_System](https://en.wikipedia.org/wiki/Domain_Name_System)
- <sup>114</sup> [https://www.allot.com/resources/BR\\_Allot\\_BusinessSecure.pdf](https://www.allot.com/resources/BR_Allot_BusinessSecure.pdf)
- <sup>115</sup> <https://www.zdnet.com/article/byod-security-warning-you-cant-do-everything-securely-with-personal-devices-says-cybersecurity-body/>
- <sup>116</sup> <https://www.allot.com/service-providers/securing-5g-network-service/>
- <sup>117</sup> Telecom providers can use the template action plan in this section, especially the business case approach, to guide their own approach. We assume in this section that hypothetical company ACME Telecom operates across the U.S. and offers conventional broadband services to 10 million customers (50 percent families and 50 percent SMB), broadband services to 50,000 small and midsize businesses and wireless service to 1 million individual subscribers. Teams reviewing this section can easily multiply our numbers by 10 (to reach 100 million broadband subscribers and 50 million wireless) or divide by 10 (to reach 1 million broadband, 5,000 SMB and 100,000 wireless subscribers).
- <sup>118</sup> To keep things simple in this section, we will use the endpoint, CPE and core solutions from Allot arranged in two simple service options. Teams reviewing this section can easily extend the sample analysis to include DDOD, 5G, DNS and other service focus options from Allot.
- <sup>119</sup> ISPs that choose to utilize the Allot platform will benefit most directly from the action plan presented here because reference is made to specific Allot service offerings. ISPs that choose to reference the action plan here in conjunction with another security solution (e.g., piecing together services or products from multiple security vendors) should also find benefit. They will need to generalize and abstract the guidance to their local situation.
- <sup>120</sup> <https://www.netpromoter.com/know/>
- <sup>121</sup> Many resources exist to help teams, including telecoms, to develop effective and accurate estimates of revenue, generally through research, surveys, review of comparable services from customers and other factors. A useful article for smaller companies can be read at <https://www.entrepreneur.com/article/76418>.
- <sup>122</sup> This is a strongly recommended first step for any telecom considering the Allot platform for security services. Determining level of potential interest helps to provide a rough gauge of funnel opportunities. Obviously, the actual purchase will be based on many factors, including monthly costs. If the service is priced too high, for example, even a customer expressing strong interest during a survey might not purchase the service. Similarly, a service priced modestly might be purchased by a customer who does not express strong interest during a survey.
- <sup>123</sup> <https://www.statista.com/statistics/216678/consolidated-revenue-of-verizon-by-quarter/>
- <sup>124</sup> The TAG Cyber analysts proposed initially a 10 percent and 12 percent increase in APRU, based on their views of potential take rates for this service. Discussion with Allot suggested that these numbers be reduced to ensure a more conservative business case. Readers might choose to increase (or decrease) the numbers on the basis of their local estimates (or actuals if the service has been put in place).
- <sup>125</sup> Depending on the negotiated deal, this might also include revenue share to the endpoint security tool provider (e.g., Bitdefender).
- <sup>126</sup> These costs will tend to be front-loaded for a telecom, especially for network and CPE engineering.
- <sup>127</sup> Many different negotiated factors will influence the revenue sharing deal between a telecom ISP, Allot and other partners. For example, the Telefonica deal referenced earlier (<https://www.costco.com/wcsstore/CostcoUSBCatalogAssetStore/Attachment/mma-costco-flyer-151205.pdf>) involved a revenue share between Allot, Telefonica and McAfee. In this sample case presented here, we will assume a flat 40 percent revenue share, with no additional sharing partners to make the math easier. This includes embedding the share costs for the Bitdefender or other endpoint security tool in the ACME Protect Plus case. The specifics of an actual negotiated deal will dictate substituting in the real numbers for the actual ROI calculation. No telecom should therefore use the 40 percent as a guide for their negotiation with Allot, since deals will certainly vary. It is used here for illustration and pedagogical purposes.
- <sup>128</sup> Dr. Amoroso of TAG Cyber designed, developed and operated the managed security service (MSS) offering within AT&T for many years during the 2000s and 2010s. Stan Quintana of TAG Cyber oversaw AT&T's MSS product marketing and delivery during the same period.

The background is a complex, abstract pattern of thin, glowing lines. The lines are primarily green, with some purple and blue accents, especially in the lower-left corner. The lines are arranged in a way that suggests a globe or a network of connections, with many lines curving and intersecting to form a dense, textured surface. The overall effect is one of dynamic energy and interconnectedness.

**DISTINGUISHED  
VENDORS**

## DISTINGUISHED VENDORS

Q 2 2 0 2 2

**W**orking with cyber security vendors is our passion. It's what we do every day. Following is a list of the Distinguished Vendors we've worked with this past three months. They are the cream of the crop in their area – and we can vouch for their expertise. While we never create quadrants or waves that rank and sort vendors (which is ridiculous), we are 100% eager to celebrate good technology and solutions when we find them. And the vendors below certainly have met that criteria.

### Abnormal

Abnormal Security protects organizations from the email attacks that matter most so they can focus on other business initiatives. Abnormal integrates with Microsoft or Google in minutes, with no disruption to the mail flow to protect you from business email compromise, supply chain fraud, account takeovers, ransomware, and other advanced email attacks.

### Acronis

Acronis integrates data protection, cybersecurity and endpoint management as a centralized, seamless all-in-one cyberdefense that unifies protection of entire data, applications and systems. Its AI-based behavioral detection engine stops malware, ransomware, cryptojacking and zero-day attacks. Advanced packets offer automated disaster recovery and enhanced protection for email, backup and cloud security.



### Arctic Security

Using external cybersecurity monitoring, Arctic Security offers an Early Warning Service that provides information about all threats in a company's network. To prevent issues before they happen, automation tools—Arctic Node and Arctic Hub—effectively collect threat intelligence in order to identify vulnerabilities and any early signs of security breaches.



Cider offers effective application security for engineering ecosystems. Ready-to-use integrations take seconds to deploy and address all requirements for releasing secure software at scale. Provided is support for all technologies—from code to deployment—as well as comprehensive, accurate analysis of frameworks and assimilations which exist in the CI/CD environment.

# TAG CYBER DISTINGUISHED VENDORS

2 0 2 2



With offices around the world, Constella Intelligence provides Digital Risk Protection Solutions that are collaborative and expansive. Services offered include all-encompassing threat detection software, identity monitoring of both surface and deep/dark webs, cyber risk intelligence defenses and thorough cyber investigation that unmask threat actors and detects hijacked and fake accounts.



Controlcase provides continuous compliance service solutions to address all aspects of IT governance, risk management and compliance management. As an ASV and QSA of PCI DSS, Controlcase, with its international staff of professional auditors, offers clients comprehensive solutions to meet objectives set forth in all federal legislation governing financial institutions.



Corelight supplies pioneering network detection and response technology to help defend sensitive, mission-critical organizations. With its enterprise-ready Zeek® and open access NDR platforms, Corelight's evidence-centric approach transforms network traffic into coherent and tangible data—easily customized and accessed—that allows companies to expand their visibility, reduce risk and improve productivity.



CyberGRX standardizes third-party cyber risk management, allowing for insights, risk prioritization, and smarter decision making across your vendor ecosystem. Driven by sophisticated data analytics and automation, real-world attack scenarios, and real-time threat intelligence, CyberGRX provides comprehensive and ongoing analysis of vendor portfolios so customers can effectively manage their cyber risk reputation.



CyCognito provides an SaaS platform that goes beyond external attack surface and vulnerability management to continuously monitor, detect and remediate risk in an organization's IT ecosystem. Founded by veterans of national intelligence agencies, CyCognito prioritizes threats based on their business impact in order to preempt security breaches and eliminate exposure.



Cyvatar offers automated and fully managed cybersecurity services for startups and small to medium-sized enterprises. Based on industry-recognized CIS 20 Critical Controls, Cyvatar's Outcome Platform accelerates the traditional install, configure and assess methodology, allowing companies to analyze, contextualize and translate complex technical data quickly and seamlessly to reach effective remediation.

# TAG CYBER DISTINGUISHED VENDORS

2 0 2 2



Deduce uses collective intelligence to protect businesses and their customers from Account Takeover and new account creation identity fraud. Its platform and developer-friendly tools combine aggregate historical user data, identity risk intelligence, and proactive alerting to deliver a robust identity and authentication solution – empowering businesses to do their part to keep their users and communities safe.



Efani is a secure mobile service with an encrypted SIM Card that protects cell phone accounts from potential SIM Swap vulnerabilities, eavesdropping and location tracking. Using rigorous identify verification and offering 24/7 tech support, Efani defends potential victims from phone hacking and cybercrimes by delinking personal information and encrypting data.



Fortinet offers advance threat protection through an integrated mesh platform security fabric that provides consistent surveillance across extended digital attack surfaces and deployments. Used by a wide range of industries from health care to finance, Fortinet ensures seamless interoperability, visibility and control, and guarantees network, application, platform and endpoint security.



Garrison's web isolation solutions deliver security for strategic digital transformation. Through the development of the world's first hardsec cloud, Garrison powers enterprise-wide secure web-access, protecting users from phishing attacks and internet-borne malware. Applying technology advanced by the National Security sector, Garrison builds flexible and scalable IT for the commercial world.



Integrating seamlessly with any SDLC, Gitguardian's code security platform scans, detects and remediates, bringing developers, security teams and cloud operations together. Using hundreds of automated, fixed sensors that scan thousands of git repositories, GitGuardian's detection engine provides companies with customized detector technology to reduce the risk of secret data exposure.



Truly iconic companies in cyber security are far-between, but HP stands out in its determination to provide a suite of products that not only support cyber security, but that actually play a key role in reducing risk to an organization. The TAG Cyber team is so grateful to HP for its kind support of our program and we appreciate the partnership.



# TAG CYBER DISTINGUISHED VENDORS

2 0 2 2

## IMMERSIVELABS

Immersive Labs is a unique cybersecurity human training platform that goes beyond generic training and certification to prepare companies internally for emerging cyber threats. Using myriad crisis simulations, gaming and creative role playing, Immersive provides practical and relevant content, teaching personnel how to become expert detectors and mitigators of cyber risk.

## ivanti

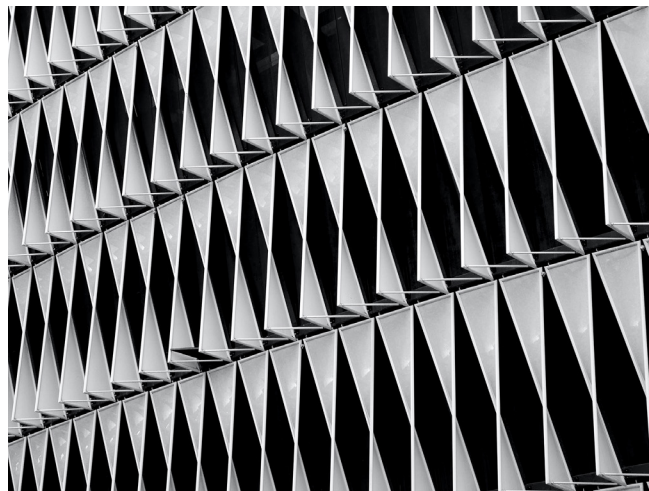
Ivanti protects IT landscapes from cloud to edge with Ivanti Neurons, a cloud-based platform that finds, repairs and protects all devices automatically wherever teams are located, giving companies the ability to streamline management by modernizing a VPN deployment and transforming into a Zero Trust design, thereby achieving fast vulnerability remediation.

## noetic

Noetic offers an intuitive, proactive approach to cybersecurity with its continuous, automated cyber asset management and controls platform. Dashboards identify and prioritize significant security insights across endpoints, users and cloud systems. This team of security industry veterans is enabling enterprises to prioritize their efforts on reducing risk on the most critical systems in their cyber environment.

## noname

With its API Security Platform, Noname Security protects APIs by identifying security risks and proactively detecting vulnerabilities, misconfigurations and design flaws before they can be exploited. While providing automatic detection and response and automatic blocking and threat remediation, the platform connects to any environment and integrates easily with existing technology.



# TAG CYBER DISTINGUISHED VENDORS

2 0 2 2



Qnext mitigates the risk of ransomware crises by offering a proprietary Zero Trust Data Access platform called FileFlex Enterprise. Built with its patented technology, FileFlex Enterprise is an overlay solution that enables any major sector organization, from healthcare, financial, to public transportation, to unify remote access, sharing, and governance of unstructured data storage across entire Hybrid-IT and Multi-Cloud infrastructures.



The Rezilion platform offers detailed, autonomous cybersecurity solutions powered by its analysis engine Unison™. Deployed in seconds as a plug-in to existing DevOps tools, Unison™ reverse-engineers and maps an entire environment, tracking inventory, provenance, runtime execution, exposure and interdependencies within each piece of code to prevent risk, drift and delays.



RiskIQ maps threat intelligence on a global scale through multiple automated discovery and continuous scanning platforms that secure an enterprise's attack surface. Composed of former NSA and intelligence officers, the RiskIQ Service team delivers precision-focused monitoring of a company's digital security, mitigating exposure by fingerprinting, detecting and thwarting cyber risk.



With its breach and attack simulation platform, SafeBreach provides a hacker's view of a company's ecosystem to help security teams switch from defense to offense. Simple to deploy and integrate, the SafeBreach platform proactively maximizes impacts of security controls: identifying and prioritizing threats, revealing vulnerabilities and improving cloud security posture.



Salt Security, with its patented API Context Engine Architecture, offers clients complete API security with the ability to stop every API attack and eliminate API vulnerabilities. The platform collects API traffic across an entire application landscape, using AI/ML and its cloud-scale data engine to reveal exposed data and enable remediation.



The Sertainty Data Privacy Platform provides unparalleled security risk mitigation. By embedding an Intelligent Module directly into data itself, Sertainty does away with unsustainable, indirect approaches to data privacy. Private information becomes tamper-resistant; self-tracking and authentication cover life cycles of digital assets, from copyright protection to registration and royalty administration.

# TAG CYBER DISTINGUISHED VENDORS

2 0 2 2



Sphere is a woman-owned company that is redefining how organizations achieve controls across their environment. Its automation platform, SPHEREboard, provides an innovative approach that starts with collection and incorporates remediation of a client's most critical data, privileged accounts, and on-premises Messaging and Office 365 assets, while simplifying reporting and automating remediation to immediately reduce risk.



Tracker Detect protects every enterprise application against insider threats using a nine step TrackerIQ process which includes detection of anomalies via a patent pending activity flow clustering engine. The platform's seamless integration provides unmatched accuracy with activity flow analytics, allowing for automatic, swift and accurate detection and response to any application.



Varonis uses Metadata Framework technology for transparent, continuous collection and analysis of information within a company's data stores and perimeter devices. Constructed by cybersecurity experts with expertise in advanced analytics, the Varonis all-in-one Data Security Platform uses automation to massively reduce risk and sophisticated detection that monitors every file to preempt cyber and ransomware attacks.



Replacing standard firewalls with state-of-the-art, hardware enforced products, Waterfall Security Solutions protects major global infrastructure control systems from sophisticated ransomware attacks. Waterfall's Unidirectional Security Gateways enable IDS sensors and security monitoring systems to connect simultaneously to both IT and OT networks, with no risk of compromise to utility or rail industry power grids.

